2022

National Cybersecurity White Paper

Published by NIS, Ministry of Science and ICT, Ministry of the Interior and Safety, Personal Information Protection Commission, Financial Services Commission, Ministry of Foreign Affairs

Contribued by KISA, NSR, FSI

Notice

Executive Summary

This white paper was written in English based on the contents of Part 1, Part 3, and Part 4 of the Korean version of the 'National Cybersecurity White Paper' published on June 20, 2022, which describes the current state of cyber security in the Republic of Korea in 2021.

Part 1, "Changes in the Cybersecurity Environment and Trends in Cyber Threats," deals with changes in the cybersecurity environment in Korea and changes in cyberattacks and threats.

Chapter 1, "Changes in the Cybersecurity Environment," covers the changing environment due to the prolonged COVID-19 pandemic.

Chapter 2, "Major Issues and Prospects for Cyber Threats," introduces five major issues.

Part 2, "Sectoral Cybersecurity Activities," gives a detailed explanation on cybersecurity policies, systems, and activities in major fields such as national information and communication network protection, digital government, critical information and communication infrastructure, information and communication services, and financial services.

Chapter 1, "National Information and Communication Network Protection" introduces cyberattack detection and blocking, incident investigation and information sharing, security management consulting and management status evaluation, security conformity verification, cryptographic module verification, security products evaluation and certification, etc.

Chapter 2, 'Digital Government,' explains the cybersecurity of digital government, software development security, and digital signature authentication.

Chapter 3, "Critical Information and Communication Infrastructure," deals with the protection promotion system for major information and communication infrastructure, main activities, and cases of domestic and international infringement incidents.

Chapter 4, "Information and Communication Services," examines infringement incident response and prevention activities, cybersecurity-related systems, and convergence security.

Chapter 5, "Financial Services," looks into financial service cybersecurity, cyber attack responses and information sharing in the financial sector, and security evaluation and inspection on financial IT and electronic finance/fintech.

Part 3, "Create a Foundation for Cybersecurity," deals with cybersecurity industry development, development of cybersecurity technology, cybersecurity manpower training, personal information protection, cybersecurity for the general-public, and international cooperation.

Chapter 1, "Cybersecurity Industry Promotion," investigates the current status of the cybersecurity industry and various policies and systems to promote the industry.

Chapter 2, "Development of Cybersecurity Technology," explains the status of the development of core technology and commercial technology.

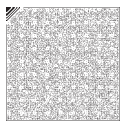
Chapter 3, "Cybersecurity Workforce," introduces the training of manpower through regular and specialized training courses and the cybersecurity certification system.

Chapter 4, "Personal Information Protection," covers policies that have been implemented to strengthen personal information protection.

Chapter 5, "Cybersecurity for General-public," examines cybersecurity consultation services and processing, and awareness-raising activities.

Chapter 6, "International Cooperation," deals with the contents of cybersecurity diplomacy and international cooperation activities related to cybersecurity.

CONTENTS

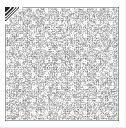


Part 3
Create Cybersecurity Environment

Table List

Figure List

Figure List



Part 1

Cybersecurity Environment Changes & Threat Trends

Chapter 1

Cybersecurity Environment Changes

As the COVID-19 pandemic has lasted longer than we expected, so did the non-face-to-face work environment that has become our daily life. The working environment has been changed to work-from-home or remote work, and the meetings use video conferences. As such, a social change triggered by COVID-19 acted as a catalyst for digital transformation, and as the boundary becomes blurred between the traditional Operational Technology (OT) industry and ICT, cybersecurity also expanded.

The digital transformation is faster than we expected and caused concerns and complaints such as online security vulnerabilities, malicious programs, personal information breaches, and privacy. Many companies adopted work-from-home or remote work use infrastructures of clouds, SaaS, and VPN/VDI, but the security threats related thereto are insufficient.

In addition, due to the convergence of ICT and the manufacturing industry, cyberattacks on the entire industry have increased, and to prepare a new type of convergence security strategy is in urgent demand. The ransomware attack on Colonial Pipeline, an American oil pipeline company, and the hacking of a water supply facility at Oldsmar, Florida, which occurred in 2021, showed that cyberattacks can cause not just system malfunction but physical damage such as gas supply disruption and water supply poisoning. These cases suggested that the attacks targeting OT systems could have greater impacts than intended, and to raise readiness by double-checking the vulnerabilities of the current OT environment security.

The expanding digital environment leads to the daily use of new ICT technologies, which became the new basis of systems and services, and also bring more concerns about cyberattacks on enterprise systems and breaches of personal/financial information collected and stored.

We are facing a new Untact (contact-free) digital environment, as a virtual environment is created to connect humans and society, with the development of networks (5G/6G), platforms, and IoT. Metaverse created a new communication method and culture originated by the MZ generation, who express "me" using virtual economy and avatars. However, there are also social problems that the minors are exposed to violent materials and pornography, and digital asset infringement, so the role of the government is being emphasized to prevent these problems.

Moreover, all user devices are connected to advanced networks, and information is shared between users and users (P2P), and users and companies (P2C), however, concerns arise about an excessive collection of personal information and privacy exposure, e.g., expanding information sharing for the prevention of infectious diseases, CCTV, and real-time information collection and analysis in virtual environments such as metaverse and digital twin.

The traditional industrial structure is changing as the entire industry is going digital, the Untact economy is expanding, and the virtual economy continues to grow, cybersecurity is becoming more highlighted throughout the economy. Technical solutions will continue to be used to meet non-face-to-face demands in diverse sectors such as medical care and education and will be accelerated to combine with core elements of the 4th industrial revolution.

As such, the government role is being emphasized more than ever due to the changes in the public/administrative sector, such as accelerating government-led digital transformation, digital-based political activities, and the transition from traditional government to platform government after the COVID-19 outbreak. The government should prepare a mid-to-long-term cyber response strategy that includes technological innovations such as cutting-edge security technologies using big data and AI so that the emerging ICT technologies will be adopted by our society, which will be the core force to drive and change our future society.

Chapter 2

Cyber Threat Issues and Foresights

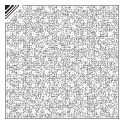
A. Hacking Threats Increase on work-from-home/remote work

The COVID-19 lasted longer and the work-from-home/remote work is increasing, so as the related threats. According to a survey conducted by global security company Thales to the executives in charge of global IT and data security, 43% responded that they experienced a security breach in 2021, and among them, the case of security breach through malware was the highest, 54%. Despite these increased security threats, about 46% of responding companies said their security infrastructure is not well-prepared for work-from-home and remote work caused by COVID-19.

The vulnerable personal devices are gaining more access, and cyberattacks such as phishing and ransomware are also on the rise, most security experts have raised their voices about the need to prepare for related security threats. If remote workers do not implement the minimum security measures required by the company, it can cause serious damage not only to individuals but also to companies.

B. Spear Phishing Persists

Spear phishing attack by e-mail is an old attack technique, but they are still effective and threatening. Spear phishing attacks continue to be found at the initial stage of a security incident, and through this, it infiltrates the company's internal network and takes over the system, causing serious damage such as information breach.



Individual awareness and attention to phishing e-mails have increased through corporate training and education, however, attackers also collect information through various channels such as social media and portals about topics that the target of attack may be interested in, such as political issues, social issues, and corporate information, and use them as attack resources to induce opening of phishing emails.

Recently, attackers are practically using more sophisticatedly crafted spear phishing emails to infiltrate into the company, e.g., by writing and sending the business context-based texts and attachments of the emails.

Spear phishing emails are ongoing cyber threats that continue to occur even at this moment and are expected to evolve into various content and more sophisticated methods in the future.

C. Social Chaos by Ransomware and Social Infrastructures Attacks

The development of information and communication technology has improved national development and people's living standards by changing the cyber environment more conveniently and efficiently. Cyberspace continues to expand in our daily life as activities across the country, including individuals, businesses, and governments, are connected to the Internet. However, this also means that the target and ramifications of cyber attacks can extend to the entire country, not to individuals or specific organizations.

State targeted cyberattack attempts on the government and national critical infrastructures are in fact steadily occurring, and the frequency of success is also increasing. For example, in May 2021, a ransomware attack by the hacking organization DarkSide targeting the Colonial Pipeline, an American oil pipeline company, paralyzed the system, temporarily halting the supply of gasoline in the southeastern United States. Around the same time, some systems of JBS Food, the world's largest meat processing company in Australia, were attacked by ransomware and paralyzed. In Korea, there have also been situations where the computer network of a manufacturer was paralyzed by a ransomware attack.

In October 2021, the U.S. State Department announced a plan to establish the Bureau of Cyberspace and Digital Policy to immediately respond to cyber threats such as ransomware. This means that the state is considering defining a cyberattack as a

security threat to the state rather than a simple security incident.

Korea has also announced such a keynote through the '2019 National Cybersecurity Strategy' and is pursuing related major tasks, and has enacted legislation to include cyber security in the scope of the National Intelligence Service.

Considering that cyberattacks are asymmetric weapons, the importance of cybersecurity is further emphasized. Therefore, cyber security should be practiced with a sense of security, and we should all make efforts to identify and check abnormal symptoms in advance.

D. Large-Scale Cyber Supply Chain Attacks Increase through Open Source

Software supply chain attacks are not new cyber threats. However, supply chain attacks that exploit the trust relationship between software vendors and customers are one of the most difficult types of attacks to prevent.

Utilizing open source software that anyone can access and freely use is very important to increase development efficiency. However, in November 2021, when the remote executable vulnerability of the open source Log4j, which is used as a function to collect logs in the JAVA development environment, became known, security officials and developers became nervous.

In the case of Log4j, the target of the application is wide and the attack range using vulnerabilities also includes both the server and the client, so it is difficult to accurately check the impact range, so there was a limit to rapid response.

In responding to Log4j vulnerabilities, it is most important to 'check whether Log4j is used among operating services, solutions, and programs'. However, since Log4j is an open source library widely used for JAVA-based program development, it is not easy to find the target that actually uses the library due to the complicated process of checking the distribution contents of the solution being used or the program manufacturer.

As such, although using open source helps to perform development efficiently, it is necessary to be careful when using it because it can pose a serious threat to security.

E. Insider Credentials Stealing Attack and Zero Trust Architecture Demand Increase

Due to COVID-19, digital transformation has been implemented rapidly in various fields, and network boundaries such as cloud computing and the increase of IoT devices are also continuously expanding. In addition, due to the expansion of workspaces such as remote work, the devices connected to the corporate network have been diversified, and the identification, authentication, and accordingly, approval processes have become very important. However, recently, there have been an increasing number of incidents in which internal network users are implicitly trusted, such as by stealing the authority of an insider. In fact, in the first half of 2021, the industry with the most incidents was the manufacturing sector (29.5%). The number of attacks to take over insider accounts, mainly credential stuffing attack and exploiting VPN vulnerabilities, are increasing. As such, the existing network boundary-based security methods (firewalls, VPNs, etc.) clearly show the limits of insider control, and the need to introduce Zero Trust Architecture that identifies and authenticates all targets and grants appropriate rights has further increased.

Zero Trust refers to a security activity that grants minimum rights to users and devices, and continuously performs authentication and authorization, assuming a network environment in which reliability is not guaranteed. In August 2020, the National Institute of Standards and Technology (NIST) announced 'Zero Trust Architecture', and in May 2021, promoted cybersecurity modernization through the 'Executive Order on Improving the Nation's Cybersecurity' while adopting a Zero Trust Architecture as a base technology.

In order to respond to new security paradigms such as cloud and contact-free environments, the Korean government is also planning to introduce Zero Trust Architecture to national critical information and communication infrastructures and public institutions. In addition, the government plans to prepare a strategy for the introduction and deployment of Zero Trust Architecture in the private sector as well.

Part 2

Cybersecurity Activities by Sectors

Chapter 1

National Information and Communication Network Security

Section 1 Cyberattack Detection and Response

The director of the National Intelligence Service (NIS) builds security operation centers/systems and operates at the government level, to immediately detect and respond to cyberattacks and threats, by Article 14 (1) and (3) of the Cybersecurity Affairs Regulations, and conducts security operation for central administrative government agencies using the system.

The heads of the central administrative agencies, local governments, and public institutions develop and operate security operation centers to detect and analyze cyber threats in real-time by Article 14 (2) of the Cybersecurity Affairs Regulations.

The security operation structure for government and public sector organizations is built on three layers: agency-level security monitoring (government and public organizations); sector-level security monitoring (central administrative agency); and national security monitoring (the National Cyber Security Center, NCSC). The National Cyber Security Center (NCSC) plays the role of detecting and responding to cyber threats that threaten national security and distributes the cyber threat detection techniques to the agency/sector network security monitoring centers.

The central administrative agency operates 44 network security monitoring centers, providing uninterrupted security monitoring 24/7 for the information and communications networks of relevant institutions and affiliated organizations. The sectoral network security monitoring centers detect and respond to cyber threats on information systems, information communications networks, and data held by the relevant national and public institutions to contain the damage. Four central administrative agencies, the Ministry of Patriots and Veterans Affairs, the Ministry of Personnel Management, the Ministry of Government Legislation, and the National Agency for Administrative City Construction, were unable to operate their own security monitoring center due to their organizational size, etc., gathered opinions on the establishment of a joint security monitoring center. Receiving technical support from the National Intelligence Service, they established a joint security monitoring center in October 2021. This is evaluated as an excellent case of inter-agency security monitoring collaboration. Meanwhile, it is necessary to have professional human resources and facilities for security monitoring. If necessary, the professionals from the specialized company designated by the Minister of Science and ICT may work together.

The NIS monitors cyber threats in real-time and promptly shares the threat intelligence with the relevant organization to minimize adverse outcomes. It shares the intelligence in real-time when there is relevance with agency/sector network security monitoring centers to achieve systematical responses at the national level.

The NCSC holds a workshop twice a year to facilitate productive cooperation. Moreover, it also presents the quarterly private-public-military sector workshop for information security companies in the private sector, the Korea Internet & Security Agency (KISA), and the Ministry of National Defense. However, due to the COVID-19 pandemic that has hit the world since 2020, only the Security Monitoring Center workshop was held online once a year to share the latest security monitoring policies and technologies.

Table 2-1-1-1 Operation of Network Security Monitoring Centers

Field	Responsible organization	Performing organization
State affairs	Ministry for Government Policy Coordination	Ministry for Government Policy Coordination Cybersecurity Center
Inspection	The Board of Audit and Inspection of Korea	The Board of Audit and Inspection of Korea Cybersecurity Center
Finance	Financial Services Commission	Financial Security Institute
National rights and interests	Anti-Corruption & Civil Rights Commission	Anti-Corruption & Civil Rights Commission Cybersecurity Center
Fair trade	Fair Trade Commission	Fair Trade Commission Cybersecurity Center
Financial affairs	Ministry of Economy and Finance	Economy and Finance Cybersecurity Center
Education	Ministry of Education	Ministry of Education Cybersecurity Center
Communication/ Science	Ministry of Science and ICT	Ministry of Science and ICT Cybersecurity Center
		Korea Internet & Security Agency (KISA) CERT
		Science and Technology Cybersecurity Center
Diplomacy	Ministry of Foreign Affairs	Foreign Affairs Cybersecurity Center
Unification	Ministry of Unification	Unification Cybersecurity Center
Legal affairs	Ministry of Justice	Justice Cybersecurity Center
National defense	Ministry of National Defense	R.O.K. Cyber Command
Administration	Ministry of Interior and Safety	National Information Resource Service (Daejeon)
		National Information Resource Service (Gwangju)
		Government Computer Emergency Response Team (G-CERT)
		Ministry of Interior and Safety Network Security Monitoring Center
Culture	Ministry of Culture, Sports and Tourism	Ministry of Culture, Sports and Tourism Cybersecurity Center
	Culture Heritage Administration	Culture Heritage Administration Cybersecurity Center
Agriculture and Food	Ministry of Agriculture, Food and Rural Affairs	Ministry of Agriculture, Food and Rural Affairs Cybersecurity Center
Energy	Ministry of Trade, Industry and Energy	Ministry of Trade, Industry and Energy Cybersecurity Center
Health care	Ministry of Health and Welfare	Ministry of Health and Welfare Cybersecurity Center
Environment	Ministry of Environment	Ministry of Environment Cybersecurity Center
Labor	Ministry of Employment and Labor	Ministry of Employment and Labor Cybersecurity Center
Land and transport	Ministry of Land, Infrastructure and Transport	Ministry of Land, Infrastructure and Transport Cybersecurity Center

Field	Responsible organization	Performing organization
Ocean	Ministry of Oceans and Fisheries	Ministry of Oceans and Fisheries Cybersecurity Center
	Korea Coast Guard	Korea Coast Guard Cybersecurity Center
Small and medium business	Ministry of SMEs and Startups	Ministry of SMEs and Startups Cybersecurity Center
National tax	National Tax Service	National Tax Service Cybersecurity Center
Customs	Korea Customs Service	Korea Customs Service Network Security Monitoring Center
Procurement	Public Procurement Service	Public Procurement Service Cybersecurity Center
Statistics	Statistics Korea	Statistics Korea Cyber Network Security Monitoring Center
Prosecution	Supreme Prosecutor's Office Republic of Korea	Supreme Prosecutor's Office Republic of Korea Cybersecurity Center
Military service	Military Manpower Administration	Military Manpower Administration Cybersecurity Center
Defense industry	Defense Acquisition Program Administration	Defense industry Operations Center
Safety	Korean National Police Agency	Police Computer Security Center
Fire fighting	National Fire Agency	National Fire Agency Cybersecurity Center
Rural development	Rural Development Administration	Rural Development Administration Cybersecurity Center
Forest	Korea Forest Service	Korea Forest Service Cybersecurity Center
Patent	Korean Intellectual Property Office	Korean Intellectual Property Office Security Operations Center
Weather	Korea Meteorological Administration	Korea Meteorological Administration Cybersecurity Center
Food and medicine	Ministry of Food and Drug Safety	Ministry of Food and Drug Safety Cybersecurity Center
Collaboration of agencies	Ministry of Patriots and Veterans Affairs, Ministry of Personnel Management, Ministry of Government Legislation, and National Agency for Administrative City Construction,	Joint Cyber Security Center

The NCSC maintains a rapid response system such as information sharing and situation notice with each security monitoring center. In addition, in order to cope with new cyber threats, it is working with each security monitoring center by continuously upgrading the monitoring system and expanding its distribution. In particular, it is focusing on developing detection technology using Artificial

Intelligence (AI) and big data technology and applying it to front-line organizations. Furthermore, to properly respond to the trend of cyber threat packets being encrypted, it is optimizing detection techniques according to the changing attack patterns, such as encouraging organizations at various levels to install visualization equipment for monitoring encrypted packets.

Section 2 Incident Analysis and Information Sharing

The NIS takes the role of national cyber incident response and analysis of state-sponsored hacking groups in accordance with Article 5 (2) of the 「National Intelligence Service Act」 and cyber adversary profiling and root cause analysis of cyber threats against central administrative agencies in accordance with Article 4 (1) 4 of the 「National Intelligence Service Act」 and Article 16 of the 「Regulations on Management of Cyber Security Affairs」.

Adversaries who are targeting high-value assets like government organizations prefer to use multi-staged attack infrastructure. To evade the tracing of its origination, they set staging servers by exploiting domestic web servers or locating them overseas out of governmental jurisdiction. NIS maintains a vigilant information exchange and technical cooperation of novel attack techniques and incident response skills with domestic and foreign organizations.

Major cases that occurred in 2021 include a hacking incident that exploited the remote working system (VPN) vulnerability, an incident in which major domestic companies in the defense industry were hacked, and an incident response to the hacking of IoT devices.

The first case was about exploiting the vulnerability of the remote work system. The hacker infiltrated the Korea Atomic Energy Research Institute and a defense company through a remote work system with poor security. The National Intelligence Service blocked the spread of damage by recognizing related content and responding quickly to reports from the related agencies. The NIS also identified the cause of the hacking incident, such as the use of the initial password for the remote work system, sharing

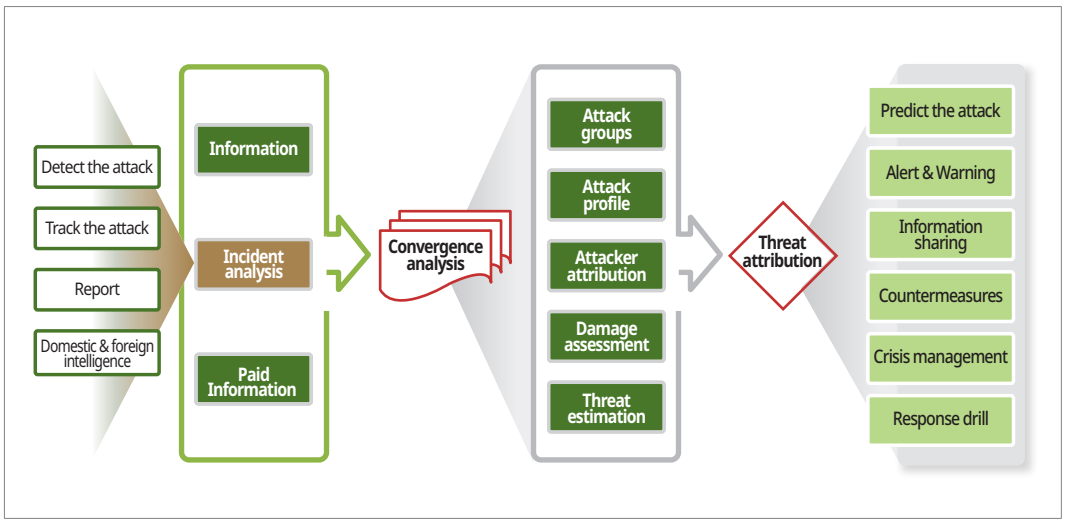
relevant information with the manufacturer, distributing the information to the public, private and military sectors, and introducing the emergency patch through the National Cyber Threat Intelligence (NCTI).

In the second case, the victim was a major defense company. In October 2021, when an unidentified hacker infiltrated a domestic defense company and demanded a large sum of money, the NIS identified the hacking route together with related organizations and investigated the contents of the leaked data. In November, the NIS confirmed that the email account of an employee of a domestic defense company was hacked, conducted a joint investigation, and took security measures to prevent further damage. If the security measures were delayed, it could lead to the leakage of defense technology and military secrets. This is because when a defense company that has key data such as defense technologies and military secrets is hacked, it would cause great losses not only for the victim companies but also for the country.

The third case was initiated by international information cooperation on identifying and responding to IoT facility hacking such as apartment facility control systems. In November 2021, the National Intelligence Service was notified by a foreign partner agency that a "Korea-based IP attempted a cyberattack on our institution," and found that domestic network-attached storage (NAS) equipment and domestic apartment and building facility control systems were hacked, and abused as a waypoint to attack Internet servers in 40 countries. In response, the NIS shared threat information with security companies, jointly checked for similar damages, and blocked the spread of damage through security measures. In addition, the NIS shared the malicious code with multiple countries which was discovered during the course of investigation by foreign intelligence cooperation organizations to prevent further hacking damage.

The incident analysis process includes analyzing attack techniques, vulnerabilities, and hacking purposes by collecting evidence and reporting or analyzing malicious codes obtained from global intelligence agencies and local and overseas security companies. In addition, to detect similar cyber incidents, the pattern characteristics of malicious codes need to be identified, and detection signatures are created and shared with the national cyber threat intelligence system. To attribute the attackers, a database of attackers' profiles of various hacking groups is required. Since pinpointing attribution is impossible with single agency data, hacking groups are classified sometimes jointly with domestic investigation agencies and domestic and overseas information security companies.

Figure 2-1-2-1 Threat information analysis and the attribution process



In addition, risk management should be conducted by cross-analyzing various types of information such as security control information and investigation results to attribute the attackers, characteristics, and scale of damage, and to predict future attacks and prepare in advance. When it develops into a nationwide crisis, the NIS should hold a crisis assessment meeting.

The government established the 'Comprehensive Measures to Strengthen the National Cyber Security Posture' in April 2015, in response to the Korean Hydro & Nuclear Power Plant hacking in December 2014. The government selected the establishment of the National Cyber Threat Intelligence (NCTI) as the main task to contain the damage through rapid situational awareness and joint response by sharing information between private, public, military, and finance sectors in large-scale cyberattacks. Moreover, the government plans to develop NCI Intelligence for prompt cyber intelligence sharing among the pre-mentioned entities.

Ten major cybersecurity organizations including the Office of National Security, the Ministry of Science and ICT (MSIT), the Ministry of National Defense, and the Financial Services Commission (FSC) established an information-sharing system at the NIS in December 2015. Moreover, these organizations shared information on cyber threat assessment and prospects, cyber incidents, response status, and network security monitoring detection status by sectors like the private, the public, the military, and finance.

To increase the situational awareness of cyber threats in the public sector and to strengthen the capabilities of the state and public institutions to respond to cyber crises, this system was linked to all central administrative agencies in June 2016 and expanded to public institutions in July 2017. Moreover, in February 2018, three metropolitan governments, including Seoul, Gyeonggi-do, and Gangwon-do, began linking the information-sharing system to local governments.

The 'Intelligence Sharing Activation Taskforce' was launched in October 2017. Ten major organizations, including the Office of National Security and the NSI, participated in operating cyber threat information sharing. It facilitates information sharing in the private, public, military, and financial sectors.

The information-sharing system has a hierarchical architecture having the NIS at the top of the tree for reliable data exchange. To enhance the accessibility of the public institutions in the innovative cities, the government established a regional hub network in cooperation with the metropolitan local governments and completed a nationwide network management system.

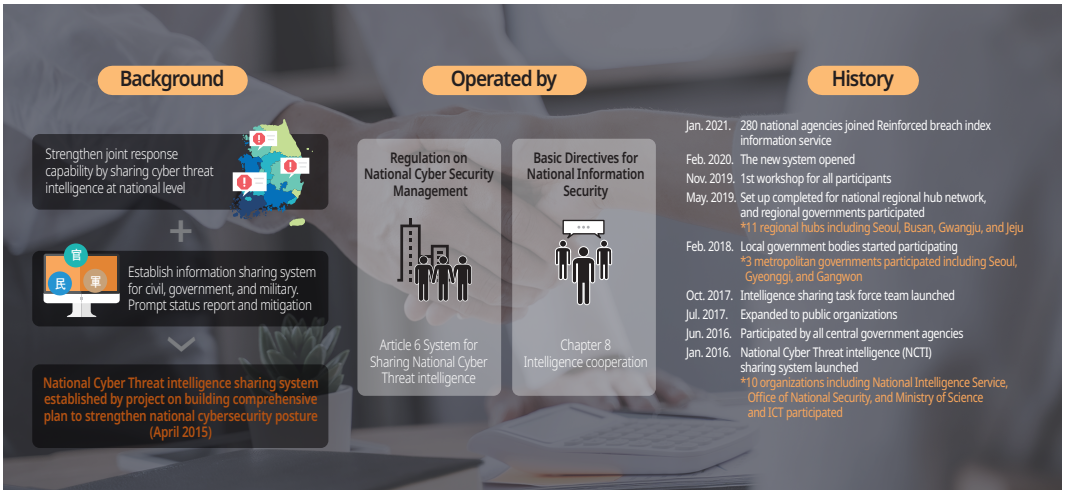
Based on this network environment, the NIS launched a new national cyber threat intelligence sharing system to facilitate information sharing between national and public institutions and strengthen the capability to deal with cyber threats. In February 2020, it opened a comprehensive cyber information portal that offers a variety of information such as threat response, preventive measures, latest trends, and statistics. And, in January 2022, the NIS released the new NCTI with enhanced breach index information service.

As of December 2021, 308 national and public institutions share cyber threat-related information through the information-sharing system. In 2021, they shared about 104,000 cases of information, and it was a 141% increase compared to about 43,000 cases of information in 2020. It is, on average, 284 cases daily, making it one of the largest information-sharing platforms in Korea.

Besides, the NIS strengthened cooperative relationships with other national and public institutions. It also holds workshops, opinion hearings, and seminars to reinforce the operation of the information-sharing system by collecting opinions from all users. In addition, the NIS conducts on-site visiting activities to improve the information-sharing process.

To reinforce the cybersecurity of the nation's mission-critical infrastructures, the NIS developed the internet-based information sharing system, Korea Cyber Threat Intelligence (KCTI), and began the service to private organizations in October 2020. Initially, 13 companies in the defense industry joined. As of January 2022, 102 companies, including the defense industry, core technology, pharmaceutical bio, and energy, have joined as members. And, it is planned to gradually expand to virtual asset exchanges and information protection companies in 2022.

Figure 2-1-2-2 Background and history of National Cyber Threat Intelligence (NCTI)



Section 3 Security Consultation and Assessment

The NIS provides security management consulting (hereinafter referred to as "security consulting") for national and public institutions by Article 4 of the 「National Intelligence Service Act」, Article 9 of 「Regulations on Cyber Security Affairs」, Article 56 of the 「Electronic Government Act」 and Article 70 of the Enforcement Decree of the same Act, Article 5 of the 「Enforcement Decree of the Public Records Management Act」, Article 97 of the 「Basic Guidelines for National Information Security」. It assesses vulnerabilities and provides consulting services so that each organization can establish information security measures. Furthermore, in accordance with Article 12 of the 「Regulation on Management of Cyber Security Affairs」, central administrative agencies and others shall conduct the diagnosis and inspection test necessary to prevent and respond to cyber-attacks and threats at least once a year.

Security consulting conducted by the NIS is done in a convergence of on-site inspection and remote inspection. The assessment specialist visits the recipient organization to evaluate security weaknesses and vulnerabilities in configuration, system/network operation, data protection, and access control. When there is a possibility of system compromise, an extensive examination for unauthorized access, data breach, and traffics to the Internet is conducted.

Remote inspection assesses the organization's web server from the Internet by penetration testing. Vulnerability factors are identified by conducting a mock attack in the same way as an actual attacker infiltrating the system by stealing administrator privileges or data theft.

After conducting on-site inspection and remote inspection, the NIS provides customized consulting services so that the recipient organization can establish and implement security measures by identifying vulnerabilities inherent in the system.

The security risk assessment is for one of the selected volunteered organizations, and the assessor and assessed set the schedule by mutual agreement. The security risk assessment comprises four steps: baseline analysis, vulnerability assessment, result analysis, and security measure establishment and recommendations.

Table 2-1-3-1 **Procedure and main contents of security risk assessment**

Step	Main Contents
Baseline analysis	• Identification of the configuration and operation status of information and communications networks that are subject to diagnosis and analysis of security systems
Vulnerability assessment	• Focused inspection on vulnerabilities such as the possibility of infiltrating the internal network through the Internet, unauthorized access to the system, and the risk of data breach through a simulated attack
Result analysis	• Vulnerability analysis and risk assessment identified as a result of the assessment
Security measure establishment and recommendations	• Notifying the results of consulting and assessment, such as establishment and recommendations for establishing security measures for each recommendations vulnerability factor.

In 2021, 35 institutions took the security risk assessment. As a result of the security assessment, using the initial administrator password without changing, using an easy-to-guess password, and keeping passwords without security measures such as encryption were identified as major vulnerabilities. After the inspection, the NIS provided technical support for patching the vulnerable system, security equipment installation, and security recommendations.

The NIS evaluates the 'information security management status' of the monitoring organizations. Throughout the evaluation, it performs a series of security tasks to harden the security postures of the organizations. The NIS manages the security postures of central administrative agencies, metropolitan local governments, and public institutions in accordance with Article 4 of the 「National Intelligence Service Act」 and Article 13 of the 「Regulation on Management of Cyber Security Affairs」, Article 56 of the 「Electronic Government Act」, Article 5 of the 「Enforcement Decree of the Public Records Management Act」, Articles 98 to 101 of the 「Basic Guidelines for National Information Security」. The inspection started with central administrative agencies in 2006, and the evaluation beneficiaries were expanded to regional metropolitan governments in 2007 and public institutions in 2009. In 2021, the inspection covered a total 195 of institutions: central administrative agencies (46), metropolitan local governments (17), and public institutions (132).

The NIS revises and complements the inspection every year to reflect changes in the security environment. Then, it notifies the relevant agency of the items, procedures, and schedule for the evaluation in advance.

Figure 2-1-3-1 Evaluation procedure of information security management status

Phase	Entity
① Agency self-assessment	Each agency
② Site inspection	National Intelligence Service
③ Additional evidence and appeal	Each agency
④ Review and confirmation of evaluation results	Evaluation Committee
⑤ Notification of evaluation results	National Intelligence Service

The evaluation process comprises five steps. First, the beneficiary institution prepares for the evaluation by pre-distributed self-evaluating worksheet. Then, the NIS reviews and verifies the appropriateness of the self-assessment. To ensure the fairness and objectivity of the verification, academic/research experts can participate in an on-site inspection. If necessary, they may ask for the submission of evidence and the interviews with the person in charge. Once completed, the beneficiary institute may file an objection along with relevant evidence. The NIS will review the complaint about the formal process of joint verification.

The 'Information Security Management Status Evaluation Committee', in which academic and research experts participated, reviews and confirms the appropriateness of the results and notifies the beneficiary institution of the final results. The recipient institute takes the results to improve the information security postures of their organization. The NIS also informs the recommendation from work to the Ministry of the Interior and Safety and the Ministry of Economic and Finance to be reflected in evaluating government affairs of national public institutions and reported to the State Council through the Ministry for Government Policy Coordination. The NIS identifies the common vulnerabilities throughout the recipient institutes and reflects them when establishing information security policies. It also closely looks into the remediation in upcoming evaluations.

Section 4 Security Compliance

1. Overview

The NIS verifies the safety of the security functions of IT products such as information security systems used by the state and public institutions. The task is done in accordance with Article 4 of the 「National Intelligence Service Act」 Article 9 of the 「Regulation on Management of Cyber Security Affairs」, Article 56 of the 「Electronic Government Act」 and Article 69 of the Enforcement Decree of the same Act, Article 5 of the 「Enforcement Decree of the Public Records Management Act」, and Articles 21, 32, 34 to 36 of the 「Basic Guidelines for National Information Security」.

The NIS commenced the security review for all information security products but the K (K1~K7) grades in April 2001. Moreover, it started information security technology evaluation for Common Criteria(CC) certified products outside the scope of the criteria like security and encryption in January 2005.

In January 2006, the NIS changed the term 'security review' to 'security verification scheme'. In August 2006, the pre-certification requirements for information security products introduced in the public sector were designated as CC certification. Before 2008, security products should go through the security verification scheme before the deployment, but it changed into the 'precondition of the security verification scheme after the deployments'. In July 2010, the security verification scheme was omitted for domestic CC-certified products. And, in October 2014, the NIS included network devices for the security verification scheme. In July 2016, to simplify the evaluation process, the accredited agency started to issue the 'information security function testing certificate', which tests whether or not the 'national security requirements' are satisfied. Since April 2019, the NIS has reinforced the issuing criteria and mandatory verification functions and added the evaluation of hardware with security requirements.

In January 2020, the term 'issuance of security function test reports' was changed to a 'security function test' system. Meanwhile, to strengthen the security of computer networks, products that play an essential role in preventing the infection of malicious codes and the data breach have been announced to be 'pre-verification and post-deployment. In 2020, organizations at all levels were required to introduce three types of network equipment,

software-based security USBs, and virtualization management products after receiving a security function test report. Switching over is expected to occur of network data leakage prevention products and host data leakage prevention products in 2021 and inter-network data transmission products in 2022. In addition, the system was improved to have the 'list of products verified for the security requirement' posted on the information sharing system, application procedures for security conformity verification omitted for the products listed on the list, and easy deployment and operation by various agencies.

In July 2020, the exemption of safety verification was announced for products with insignificant security functions (7 types), allowing each institution to deploy these products with no condition attached.

Table 2-1-4-1 Products able to be introduced and operated autonomously without safety verification

Order	Product Type	Main Function
1	Network-based privacy protection product	Network-based personal information detection
2	Host-based privacy protection product	Host-based personal information detection
3	Network vulnerability check tool	Network vulnerability analysis and reporting
4	Host vulnerability check tool	Host vulnerability analysis and reporting
5	Harmful site blocking system	Block access to harmful sites
6	Web shell detection product	Web shell detection and isolation in the web server
7	Log management products (Limited to simple log collection products)	Collect logs from log collection target

Moreover, in September 2020, with inadequacies in the GS certification system for security requirement verification and a small number of applications, the NIS excluded the GS certification from January 2022 from the deployment requirements of the information security system. In October 2020, with many information security products having modified and installed a no longer managed Linux kernel of a lower version (2.X) from 2023, the NIS limited the use of the products with a lower version kernel.

In January 2020, the following products were included in the 'List of Verified Products', which is registered in the NCTI: products that have received domestic CC certification, products that have received international CC certification by applying the national Protection Profile (PP), products that have received a security function test report, products that have received a confirmation of performance evaluation results by conforming to the national security requirements, 'List of Verified Products'

containing products that have received GS certification in compliance with national security requirements. In December 2021, it was released along with the opening of the National Cyber Security Center website.

In June 2021, in line with the government's cloud distribution promotion policy, it was decided to defer the verification of information security products operated in the cloud until 2024. And, the pre-authentication requirements for 24 types of information security products introduced in the public sector, which were unified with CC certification in December 2012, were expanded to 'CC certification or security function test report' and applied from January 2022.

2. Verification procedure

National and public institutions planning to deploy the products with information security functions should apply for the information security function requirement verification to the NIS. The process looks into the requirement for CC certification or information security function verification. The NIS examines the information security function through the National Security Research Institute (NSR) and informs the applicant of the results. After the remediation is fully applied, the organization deploys the product to its network. In terms of the products included in the 'list of verified products' and listed on the National Cyber Security Center website, after deployment, they can be operated by submitting operation checklists, Executive Summary confirmation, and copies of certificates, with no application for security requirement verification.

3. Requirement for products deployment

A. Products with Mandatory CC certificate or security function test report

16 types of information security systems, including intrusion detection systems and intrusion prevention systems, are mandatory to acquire domestic and foreign CC certifications or security function test reports. Among those products with CC certification, four products such as virtual private network and Single Sign-On (SSO) must have verified 'cryptographic module' approved by the NIS Director.

Products on the list of verified products may be deployed without a security

requirement verification process. Except for digital multifunction printers, the products that have received CC certification but are not on the list of verified products must apply for security conformity verification after introduction.

Table 2-1-4-2 Products able to be introduced only with CC certificate or security function test report

No.	Product(Module) type	Executive Summary requirements	Remark
1	Firewall	CC certificate or security function test report	
2	web application firewall		
3	VoIP Security Product		
4	Intrusion Prevention System		
5	Wireless Intrusion Prevention Product		
6	Network access control product		
7	Wireless LAN Authentication Product		
8	Spam mail Prevention systems		
9	Smart Card		
10	Enterprise Security Management Product		
11	Mobile Device Management		
12	Operating System (Server) Access Control Product		
13	Integrated Log Management Product		
14	Patch management system		
15	DB Access Control Product		
16	Digital Multi-function Printer		
17	Single Sign On (SSO) Product	CC certificate or security function test report + verified cryptographic module	
18	Virtual private network product		
19	Digital Rights Management (DRM)		
20	DB encryption product		

Meanwhile, anti-spam, patch management, and data diode products are on the safety verified product list and may be deployed and operated without the security requirements verification. . However, from January 2022, products with GS certification cannot be newly registered on the safety verification product list, and its introduction is restricted.

B. Products able to be introduced only with one of CC certificate, performance evaluation, and security function test report

Anti-DDoS, anti-virus, and analysis tool for source code security weakness may be deployed without the procedure of security conformity verification when the products satisfy one of CC certificate, performance evaluation, and security function test report.

Table 2-1-4-3 Products that require one of CC certificate, performance evaluation, and security function test report

No.	Product(Module) type	Executive Summary requirements	Remark
1	Analysis Tool for Source Code Security Weakness	one of CC certificate, performance evaluation, and security function test report	
2	Anti-DDoS Product		
3	Anti-virus Product		

C. Products whose security function test report is the only pre-authentication requirement

11 types of software-based security USB and data leakage prevention products related to internal and external data transmission of government computer networks must obtain a security function test report.

Table 2-1-4-4 Products that require security function test report

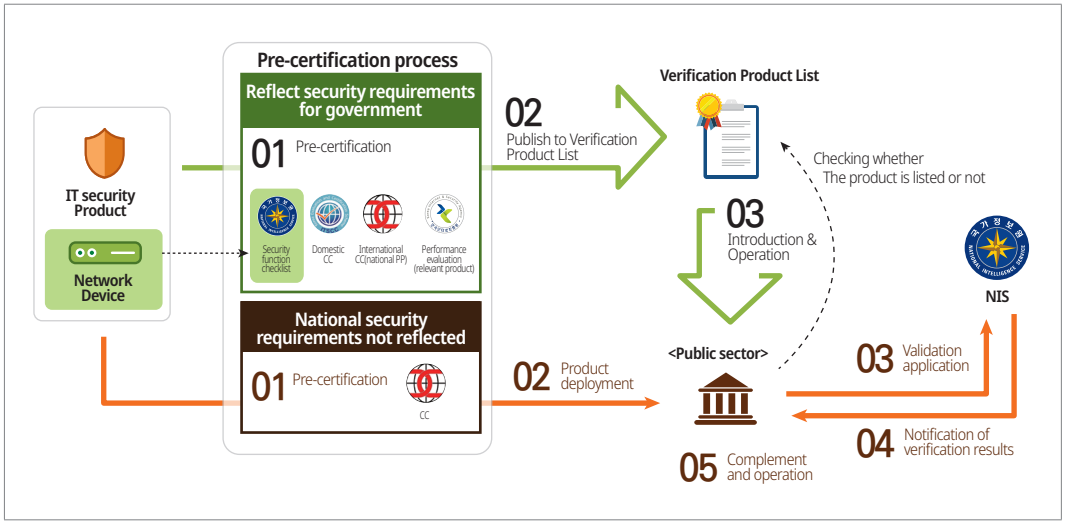
No.	Product(Module) type	Executive Summary requirements	Remark
1	Software-based secure USB product	security function test report	
2	Host Data Loss Prevention (HDLP)		
3	Network Data Loss Prevention (NDLP)		
4	Inter-Network Data Transmission Product		
5	Virtualization management product		
6	Network equipment		
7	Switches (L3, L4, L7, etc.)		
8	Router		
9	SDN controller		
10	SDN switch		
11	Other network equipment		

4. IT product deployment to national and public institutions

A. Requirements for deployment of information security and data communications products with security functions

Government and public institutions may deploy the information security and data communication products in accordance with Article 20 of the 「Basic Guidelines for National Information Security」. The followings are the products that satisfy the requirements: the products registered on the safety verification product list through pre-accredited certification tests such as CC certification, security function confirmation, and performance evaluation, and the products that did not comply with national security requirements but obtained CC certification. Moreover, the NIS director may announce the particular requirements for products that do not satisfy the pre-mentioned conditions. Deployment of products registered on the safety verification product list confirms that the organization or institute does not need the additional information security requirement certification. However, other products must undergo the process of information security verification before actual deployment and operation.

Figure 2-1-4-1 Procedures for introducing IT products by national and public institutions



B. The Internet phone and video security equipment

The VoIP phone, mobile phone, and video security product for administrative agencies must obtain TTA certification. Since January 2016, it became mandatory for the national

and public institutions to have TTA verified version 4 or higher in using the VoIP phone. The NIS recommended TTA-certified products for mobile phone and image information processing products (IP-based CCTV for facility security and management, etc.).

Section 5 Cryptographic Module Validation

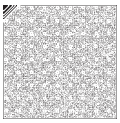
1. Overview

The NIS validates cryptographic modules' security and implementation suitability to protect not classified but sensitive data communicated and stored in the national information network. It is in accordance with Article 9 (2) and (3) of the 「Regulation on Management of Cyber Security Affairs」, Article 56 of the 「Electronic Government Act」 and Article 69 of the Enforcement Decree of the same Act, and the 「Guidelines for Testing and Validation of Cryptographic Modules」.

Software, firmware, hardware, or any combination of the technologies above and cryptographic algorithm (Table 3-1-5-1) must comply with the cryptographic module security requirements (KS X ISO/IEC 19790:2015). Requirement satisfaction should go through the cryptographic module test requirements (KS X ISO/IEC 24759:2015).

The NIS had started cryptographic module validation in 2005 and revised it in 2015 for the cryptographic module security requirements and test requirements. The Korea Internet & Security Agency (KISA) joined the accredited cryptographic module testing agency in 2018. The NIS and KISA are the only two accredited cryptographic module testing agencies in Korea.

The NIS enacted and published the 'Cryptographic Module Test and Verification Guideline' as a guideline for the NIS (November 1, 2021) and opened a new website for 'Cryptography Module Verification' of the National Cyber Security Center. And, new menu items such as system introduction, a detailed explanation of the encryption module test/verification procedure, and Frequently Asked Questions(FAQ) were added to the website to enhance transparency and communication. In addition, the NIS developed a new test method for random number generators and improved the standards for test methodologies related to TTAK.KO-12. 0235 (Guideline for



Collection and Application of Noise Sources on Operating System) and TTAK.KO-12.0341 (Guideline for Testing Noise Sources used in Software Cryptographic Modules). By making the new test technologies for random number generators mandatory as of June 1, 2022, the ease of implementation of cryptographic modules by companies and the safety of cryptographic modules have been improved.

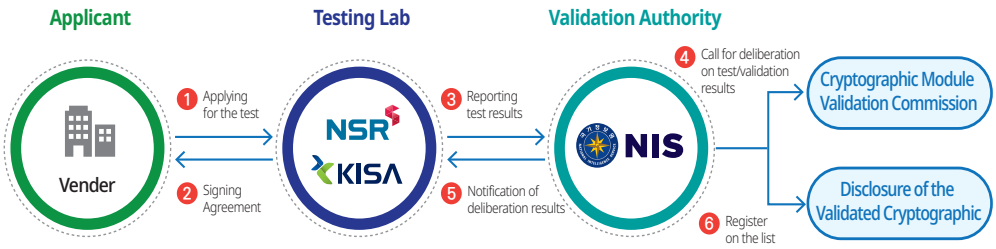
Meanwhile, in cooperation with the KISA, the NIS is operating a specialized training course for cryptographic modules for crypto-related industries and graduate schools (students). In 2021, an in-depth curriculum focusing on the implementation of cryptographic modules was additionally organized by reflecting the opinions of students in 2020 and the basic curriculum. These courses focused on the implementation of the verification target algorithm, high-level cryptographic module verification method, and interpretation of verification standards. About 200 people in the basic curriculum and 200 people in the intensive curriculum took the online courses. In addition to the specialized training for cryptographic modules, the NIS provided consulting projects for 5 small and medium-sized businesses. Through cipher module verification standard interpretation training and review of the submission, the NIS supported them to prepare and supplement documents submitted (basic and detailed design documents, test procedures and results, configuration management documents) when applying for cryptographic module tests. All five companies are currently in the process of applying for the cryptographic module test.

2. Validation System and Process

A. Cryptographic module validation system

There are two types of organizations in the cryptographic module validation process in terms of roles and responsibilities. First, as a validation organization, the NIS establishes and implements the policy, develops validation standards, and approves testing technology. It also designates, manages, supervises the testing organization, manages testing results and the list of the cryptographic modules, and holds a validation committee. The National Security Research Institute (NSR) and the Korea Internet & Security Agency (KISA) are the testing institutions that conduct cryptographic module test contracts and tests, research and development of standards and technologies related to cryptographic module tests, and consulting and education services.

Figure 2-1-5-1 Cryptographic module validation system



❶ After determining the appropriate security level of the cryptographic module, the applicant applies for a test to the testing lab.

❷ After examining the application and submitted materials, the testing lab signs an agreement with the applicant and conducts the test according to the cryptographic module verification standards

❸ After completing the test, the testing lab reports the test results to the validation authority.

❹ The validation authority reviews the results of the cryptographic module test to confirm whether they meet the verification standards or not, and the cryptographic module validation commission reviews the validity and fairness of the test/validation results.

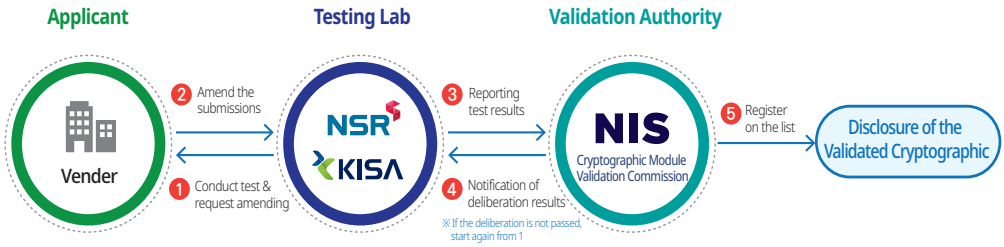
※ The validation commission is composed of experts from government, academia, and research institutes.

❺ The validation authority notifies the testing lab of the deliberation results

❻ The validation authority registers the cryptographic module that has been reviewed on the list of verified cryptographic modules.

B. Cryptographic module validation process

Figure 2-1-5-2 Cryptographic module validation process



❶ The testing lab tests the cryptographic module according to the verification standards and requests for amending from the applicant when any corrections are found in the submissions.

❷ The applicant submits to the testing lab after amending the submissions according to the amending request of the testing lab.

❸ After completing the test, the testing lab reports the test results to the validation authority, and the validation authority reviews whether the test results meet the verification standards.

❹ The validation authority deliberates and decides on the validity and fairness of the test and deliberation results in the cryptographic module validation commission, which is composed of experts from government, academia, and research institutes, and notifies the testing lab of the deliberation results.

❺ The validation authority assigns verification numbers to cryptographic modules that have been reviewed and put them on the list of verified cryptographic modules.

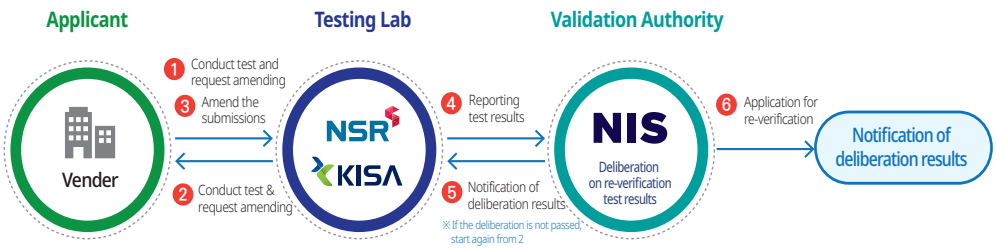
※ Testing lab can request support for the testing environment and holding briefing sessions from the applicant for smooth test procedure and understanding of submitted materials.

※ Testing lab may suspend the test agreement if the testing lab determines that the test cannot be continued due to reasons such as the applicant's delayed amendment of submitted materials without any special reason.

※ Testing lab has the authority to check the security management status of the cryptographic module development environment of the applicant.

C. Measures to be taken when the validation effect expires and the configuration is changed

Figure 2-1-5-3 **Measures to be taken when the validation effect expires and the configuration is changed**



❶ When the verification effect expires or the configuration of the cryptographic module is changed, the applicant prepares a re-verification application form and required documents and applies for re-verification to the testing institute.

❷ The testing lab tests the cryptographic module according to the verification standards and requests for amending from the applicant when any corrections are found in the submissions.

❸ The applicant submits to the testing lab after amending the submissions according to the amending request of the testing lab.

❹ After completing the test, the testing lab reports the test results to the validation authority, and the validation authority reviews whether the test results meet the verification standards.

❺ The validation authority deliberates on the validity and fairness of the test and deliberation results in the cryptographic module validation commission and notifies the testing lab of the deliberation results.

❻ The validation authority updates (or maintains) the verification numbers of the cryptographic modules that have been re-reviewed and updates the list of verified cryptographic modules.

※ Testing lab can request support for the testing environment and holding briefing sessions from the applicant for smooth test procedure and understanding of submitted materials.
※ Testing lab has the authority to check the security management status of the cryptographic module development environment of the applicant for re-verification.
※ Testing lab may suspend the test agreement if the testing lab determines that the test cannot be continued due to reasons such as the applicant's delayed amendment of submitted materials without any special reason.
※ Regarding the application period, if an organization applies for re-verification to extend the validation effect of the cryptographic module, the organization must apply 6 months before the expiration of the validation effect.
※ If serious vulnerabilities are found in the verified cryptographic module, re-verification may be performed at the request of the testing institution. In this case, the applicant organization shall immediately notify the organization that intends to introduce the cryptographic module of the vulnerability and may suspend the validation of the cryptographic module until the vulnerability is corrected.

3. Approved Cryptographic algorithms

The validation authority chooses a cryptographic algorithm that is subject to the validation. The process undergoes safety (security strength), efficiency, standardization, domestic and international cryptography policy, incompatibility, and intellectual property rights. The cryptographic algorithm, including block ciphers, hash functions, message authentication codes, random number generators, essential establishment, public-key cryptography, digital signatures, and key derivation functions, are classified into 23 items of eight types. They must satisfy cryptographic strength of more than 112 bits.

Figure 2-1-5-4 Approved cryptographic algorithms

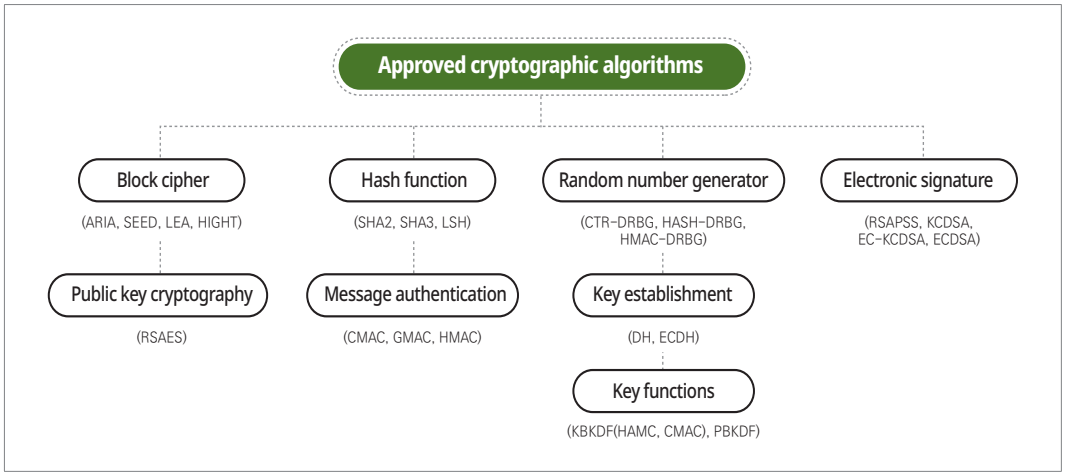


Table 2-1-5-1 Approved cryptographic algorithms

Classification		Cryptographic algorithm
Block cipher and operational mode		• ARIA, SEED, LEA, HIGHT (Key length 112 bits or more)
		• ECB, CBC, OFB, CFB, CTR, CCM, GCM
Hash function		• SHA-2 (SHA-224/256/384/512), SHA-3 (SHA3-224/256/384/512), LSH (LSH-224/256/384/512/512-224/512-256)
Message Authentication code	Hash function based	• Message Authentication code
	Block cipher based	• GMAC, CMAC
Random number generator	Hash / HMAC based	• Random number generator
	Block cipher based	• CTR_DRBG
Public key cryptography		• RSAES (Public key length: 2048/3072, Hash function: SHA-224/256)
Electronic signature		• RSA-PSS (Public key length: 2048/3072, Hash function: SHA-224/256) • KCDSA (Public key length: 2048/3072, Private key length: 224/256, Hash function: SHA-224/256) • EC-KCDSA (P-224, P-256, B-233, B-283, K-233, K-283, Hash function: SHA-224/256) • ECDSA (P-224, P-256, B-233, B-283, K-233, K-283, Hash function: SHA-224/256)
Key establishment		• DH (Public key length: 2048/3072, Private key length: 224/256) • ECDH (P-224, P-256, B-233, B-283, K-233, K-283)
Key functions		• KBKDF (HMAC, CMAC) • PBKDF (HMAC)

4. Status of validated cryptographic modules

There is a list of validated cryptographic modules on the NIS web pages (https:// www. nis.go.kr:4016/AF/1_7_3_3/list.do) and the National Cyber Security Center website (https://www.ncsc.go.kr:4018/ PageLink.do). The list includes the cryptographic module name, module type, validation date, expiration date, security level, security policy document, and configuration data information. From 2005 to January 2022, a total of 309 cryptographic modules have been verified. Government organizations and public institutes can use a total of 75 cryptographic modules of which validations are effective, including 58 software, eight firmware, and nine hardware.

Table 2-1-5-2 **Status of validated cryptographic module**

(Unit of measurement: cases)

		2015	2016	2017	2018	2019	2020	2021	Total
Types of test	New	5	7	5	9	9	13	14	62
	Revalidation	14	16	14	13	16	14	15	102
Total		19	23	19	22	25	27	29	164

Section 6 Security Products Evaluation and Certification

1. Overview

The NIS evaluates and certifies the information security products by Article 58 of the 「Basic Act on Intelligence Informatization」, Article 51 of the Enforcement Decree of the same Act, and the 「Guidelines for Evaluation and Certification of Information Security Systems」 (notification of the Ministry of Science and ICT). It is for the government and public institutions to have secured information security products.

In 1998, it began full-scale evaluation and certification by developing and announcing the evaluation criteria (K criteria) customized for domestic entities. The subject of the evaluation expanded to intrusion prevention system in 1998, intrusion detection system in 2000, virtual private network in 2002, and access control in the operating system, fingerprint authentication system, and smartcard system in 2003.

The NIS unified the evaluation criteria to CC and expanded to all information security products for diversifying security functions and unifying security products. The NIS discontinued K-criteria in 2006.

In 2007, the CC evaluation, which was originally only for global products, diversified into domestic and international purposes, expediting the processing time and lessening the financial burdens for local medium and small-sized security vendors. The procedures became further simplified in 2010.

The NIS selected 26 products, subject to evaluation and certification process, for government and public institutions in 2011. To promote the quality improvement of the information security products, in February 2012, the NIS published requirements for the domestic information security products and set a three-year expiration date for the certification. In November 2012, the NIS transferred IT Security Certification Center to the National Security Research Institute (NSR). The NIS included the 28 smartphone security management and source code vulnerability assessment products subject to evaluation and certification.

The NIS transferred CC certification procedures to the Ministry of Science, ICT and Future Planning in October 2014. The NIS, the Ministry of Science, ICT and Future Planning, and the IT Security Certification Center of the NSR (hereinafter referred to as the 'IT Security Certification Center') revised the products subject to the evaluation and certification. The NIS adjusted the total number of the product to 24 types in January 2016.

The government renamed the Ministry of Science, ICT and Future Planning to the Ministry of Science and ICT (MSIT) in July 2017. The MSIT and the IT Security Certification Center revised the 「Korea IT Security Evaluation and Certification Regulation」 to reflect the latest CCRA agreements and policies. The CCRA revised the CC. The IT Security Research Institute registered the NSR as an agency with intellectual property rights by acting as an editor at the time of revision in April 2017. The NIS includes a protection profile for seven types of intrusion prevention system products, Host Data Loss Prevention (HDLP), Network Data Loss Prevention (NDLP), wireless intrusion prevention system, database encryption, document encryption, and unified authentication system. It enables the NIS to evaluate and certify at the level of international standards. In January 2020, as secure USB and others are introduced

to the government and public institutions as a security function certificate, the types of information security systems that required CC certification when adopted by the government and public institutions have slightly decreased to 23 products, including intrusion detection systems.

The IT Security Certification Center proposed cPP for a multi-function printer for government and public institutions in 2018. It took the initiative in Common Criteria Development Board (CCDB) working groups reflecting requirements for national and public institutes in Korea. It also proposed CCRA common technical document for products utilizing four international standard cryptographic algorithms (SEED, HIGHT, KCDSA, EC-KCDSA), which Korea had developed, for global evaluation and certification.

The NIS updated three types of national security requirements of information protection products, including integrated security management products, DLP products, and software-based security USB products for the latest technology trends and security threats in 2018. It also included two national protection profiles for smartphone security management and a database access control system for the government and public institutions.

The IT Security Certification Center has been developing national protection profiles that require evaluation and certification since 2015. It has developed and certified national protection profiles for 17 product types, including network access control products providing global standards for evaluation and certification by 2019.

In 2019, the government made it possible for the product to have a private contract, which satisfies the national security requirements by revising the Article 26 of the Enforcement Decree of the 「Act on Contracts to which the State is a Party」, and it came into force in December of the same year.

2. Evaluation and certification system

On the basis of Common Criteria (CC), ISO/IEC 15408, evaluation and certification of information security products are conducted based on CEM (Common Evaluation Methodology, ISO/IEC 18045). The assurance level is the trustworthiness of objectivity and accuracy of the security products implementation. It is classified into EAL(Evaluation Assurance Level), and details are listed in [Table 2-1-6-1].

Table 2-1-6-1 EAL for information security products

Assurance Level	Assurance level and description
EAL1	• Functional test based on guidance documentation of the product without developer assistance
	• Vulnerability assessment focused on potential vulnerabilities in the public domain and a Basic attack potential
EAL2	• Structural test based on function testing of developer level about external interface and independent testing by evaluator
	• Vulnerability assessment focused on potential vulnerabilities in the public domain, independent vulnerability analysis, and a Basic attack potential
EAL3	• In addition to EAL2 level test, methodical test and check based on internal interface test, examination on development environment and product's configuration change system
	• Vulnerability assessment focused on potential vulnerabilities in the public domain, independent vulnerability analysis, and a Basic attack potential
EAL4	• In addition to EAL3 level test, methodical test and review based on source code of implementation result and examination on development tools
	• Vulnerability assessment focused on potential vulnerabilities in design description and implementation result, independent vulnerability analysis, and an Enhanced-Basic attack potential
EAL5~7	• Semi-formal or formal verification based on more rigorous and detailed verification of product's design configuration change system
	• Vulnerability assessment focused on more comprehensive independent analysis of architecture structure, structured representation of implementation or formal representation using expert equipment and expert knowledge, and an Expert level or a higher attack potential

The information security products evaluation and certification entities are divided into policy organizations, certification organizations, evaluation organizations, and accreditation organizations according to their roles and responsibilities.

The policy organization, the Ministry of Science and ICT, defines national policies for certification of information security products, establishes regulations and

standards for evaluation and certification, manages the certification organizations, and establishes and announces guidelines for evaluation and certification.

The certification organization, the IT Security Certification Center, issues certification reports and certificates after confirming the evaluation organization's appropriateness and validity and performs evaluation organization management like granting evaluator qualifications and designating evaluation institutions. It also oversees international cooperation like CCRA committee activities and examination of member countries.

The designated evaluation organization, the KISA, and six other organizations approved by the certification agency (KoSyAs, KSEL, TTA, KOIST, KTC, KTR) evaluate information security products.

The accreditation organization, the Korean Agency for Technology and Standards (KATS), plays the role of recognizing a testing organization that wishes to be approved as the evaluation organization by a certification organization as an official testing agency by international standards.

Figure 2-1-6-1 **Information security product's evaluation and certification system**

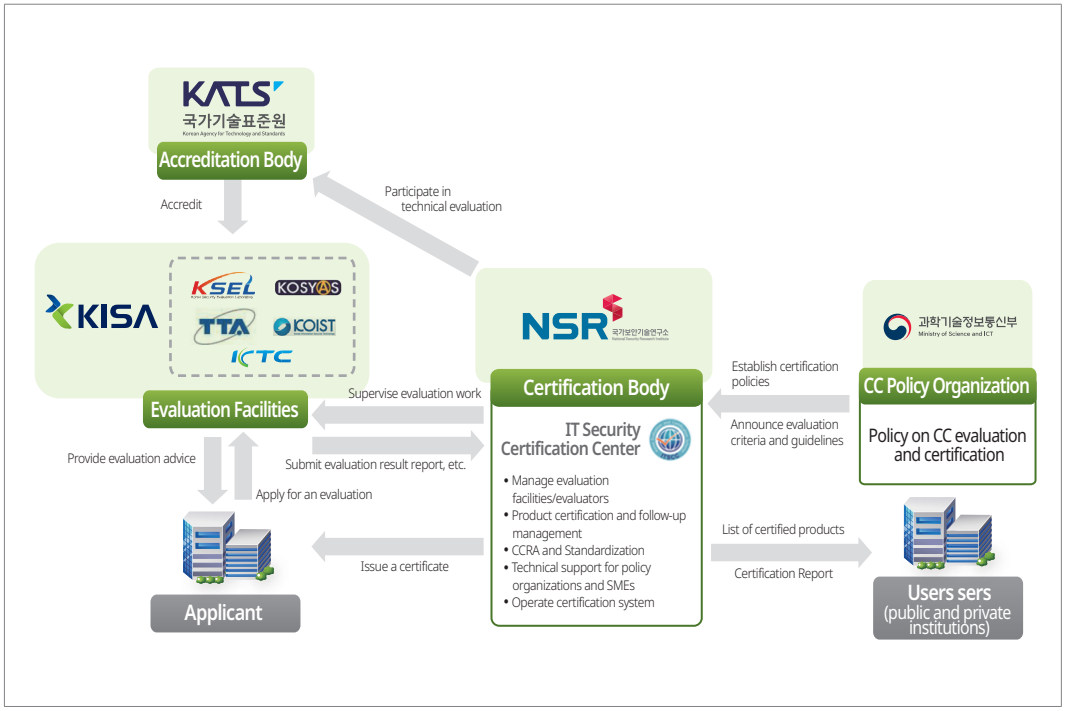
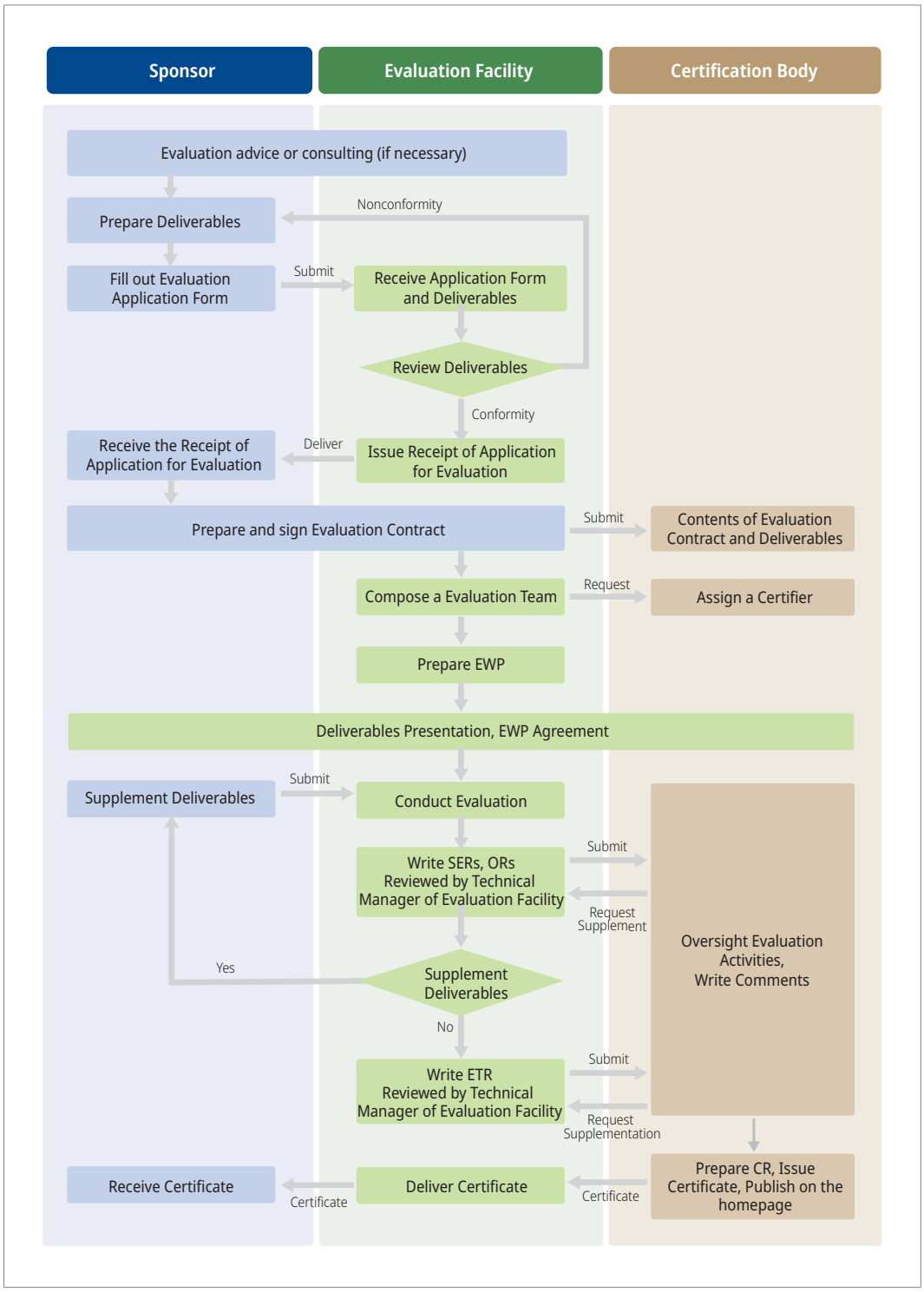


Table 2-1-6-2 **CC evaluation facilities accredited by IT Security Certification Center**

Designation	Founding date	Website
Korea Internet & Security Agency	February, 1998	http://www.kisa.or.kr
Korea System Assurance, Inc	August, 2007	http://www.kosyas.com
Korea Security Evaluation Laboratory	August, 2009	http://www.ksel.co.kr
Telecommunications Technology Association	October, 2009	http://www.tta.or.kr
Korea Testing & Research Institute	October, 2010	http://www.ktr.or.kr
Korea Information Security Technology	April, 2014	http://www.koist.kr
Korea Testing Certification Institute	December, 2014	http://www.ktc.re.kr

The information security product's evaluation and certification processes are divided into a preparation stage, an evaluation/certification stage, and a finish stage in the information security product evaluation/certification process. In the preparation stage, it reviews evaluation applications and submissions. In the evaluation/certification stage, it finalizes an evaluation contract. The organization performs evaluations, including evaluations of proposals such as design error verification, security function tests, and vulnerability verification to verify the safety and reliability of the information protection product. The certifying organization reviews and deliberates on the evaluation results. In the final stage, the certification organization prepares the certification report and issues the certification to the applicant for evaluation.

Figure 2-1-6-2 Evaluation and certification procedure of Information security products



3. Evaluation and certification status

As of December 31, 2021, the number of information security products with CC certification summed up to 1,116, of which 960 were for domestic certification schemes and 156 for international use, including products with canceled certification for discovered security vulnerabilities and expired validation date products. For domestic CC-certified products, network security equipment like firewalls, intrusion prevention systems, and access control systems account for more than half of the total.

Table 2-1-6-3 **Status of certified products by EAL**

Assurance Level		2003~2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
EAL1	For international use							2	3	1	1	1	1	9
	For domestic use													0
EAL1+	For international use							5	7	2	5	1		20
	For domestic use													0
EAL2	For international use				1		2		2		1			6
	For domestic use	48	36	28	14	43	42	33	36	24	23	32	29	388
EAL2+	For international use					1	5	2	1			1		10
	For domestic use	3	1											4
EAL3	For international use	8	1											9
	For domestic use	31	14	15	20	16	15	19	14	12	18	12	10	196
EAL3+	For international use	9		4		2								15
	For domestic use	67			2		1							70
EAL4	For international use	20	1	1	1									23
	For domestic use	69	9	23	8	26	40	22	18	16	17	30	24	301
EAL4+	For international use	11		3		1	1				1		1	18
	For domestic use		1											1
EAL5+	For international use	2	1		3	3	3		3		1	1	2	19
	For domestic use													0
PP Observance	For international use								1	3	12	6	5	27
	For domestic use													0
Total for international use		50	3	8	5	7	11	9	17	6	21	10	9	156
Total for domestic use		217	61	66	44	85	98	74	68	52	8	74	63	960
Total		267	64	74	49	92	109	83	85	58	79	84	72	1,116

Among international CC-certified products, smart card-related products like e-passports and smart card operating systems, and multi-function printers took up more than half of the total. From 2016 to 2017, it completed international CC certification for new technology like smart TV security software. After 2018, three types of encryption products (document encryption, database encryption, integrated authentication) based on national protection profiles have been certified. In the case of 2021, the number of both domestic and international CC certifications decreased compared to 2020.

4. CCRA activities

After joining the CCRA in 2006, Korea has been in effort for more international cooperation activities to be a better responsible certificate issuing member country. To do that, Korea participated in the Common Criteria Recognition Arrangement (CCRA) meetings composed of the Common Criteria Maintenance Board (CCMB), the Common Criteria Development Board (CCDB), the Common Criteria Executive Subcommittee (CCES), and the Common Criteria Management Committee (CCMC), and presented the status of evaluation and certification of domestic information security products and analyzed international evaluation technologies and evaluation policy trends.

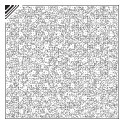
Along with the CCRA activities, the AISEC (Asian IT Security Evaluation and Certification) forum started in 2009. It aims to promote the sharing of policies and technologies related to the evaluation and certification of Asian CCRA member countries and strengthen international cooperation such as support for Asian countries to join CCRA certificate issuing countries.

The CCRA announced a vision statement in 2012 focusing on the development of cPP, a collaborative protection profile approved by multiple schemes. Accordingly, it concentrates on cPP development by forming an international technical community where vendors, evaluation facilities, certification bodies, and government agencies participate in each security technology field. In July 2014, CCRA members agreed on an amendment to the agreement with the main content of mutual recognition of cPP-based certified products. In September of the same year, 26 CCRA member states signed the revised agreement. At that time, the NIS and NSR jointly signed the revised agreement as representatives of the Korean government. Ethiopia in 2017, Poland in

Table 2-1-6-4 **CCRA Member States**

	Country	Website of the certification body
Issuers of the certificate (17 countries)	Austria	https://www.cyber.gov.au/acsc/view-all-content/programs/australasian- information-security-evaluation-program
	Canada	https://www.cyber.gc.ca
	France	http://www.ssi.gouv.fr/
	Germany	http://www.bsi.bund.de/
	India	http://www.commoncriteria-india.gov.in/
	Italy	http://www.ocsi.isticom.it/
	Japan	https://www.ipa.go.jp/security/jisec/jisec_e/
	Malaysia	http://www.cybersecurity.my/mycc
	Netherlands	https://www.tuv-nederland.nl/common-criteria/
	New Zealand	https://www.cyber.gov.au/programs/australasian-information-security- evaluation-program
	Norway	http://www.sertit.no/
	South Korea	http://itscc.kr
	Singapore	https://www.csa.gov.sg/programmes/csa-common-criteria
	Spain	https://oc.ccn.cni.es
	Sweden	https://www.fmv.se/verksamhet/ovrig-verksamhet/csec/
	Turkey	https://en.tse.org.tr/KurumsalSablon?ID=666&ParentID=2312
	United of States	https://www.niap-ccevs.org/
Recipients of the certificate (14 countries)	Austria	http://www.digitales.oesterreich.gv.at/
	Czech Republic	https://www.nukib.cz/en/
	Denmark	https://www.cfcs.dk
	Ethiopia	http://www.insa.gov.et
	Finland	https://www.ncsc.fi/
	Greece	http://www.nis.gr/
Recipients of the certificate (14 countries)	Hungary	http://www.kormany.hu/en/ministry-of-national-development
	Indonesia	https://www.bssn.go.id/idcc
	Israel	http://www.sii.org.il/
	Pakistan	http://www.commoncriteria.org.pk/
	Poland	https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo
	Qatar	http://www.motc.gov.qa/
	Slovakia	https://www.nbu.gov.sk/en/index.html
	United Kingdom	http://www.ncsc.gov.uk/

[Source: CCRA website



2018, Indonesia, and Slovakia in 2019 joined the CCRA as recipients of the certificates, and CCRA member states make up thirty-one countries in total. The thirty-one countries mutually recognize international CC certificates issued in Korea.

As of December 2021, the CCRA has approved eight international technical communities and is developing cPP for product types such as security USBs, network equipment, disk encryption, application software security, dedicated security modules, databases, bio-certification, and digital multifunction printers. In particular, since 2020, Korea has been leading the development of cPP for digital multifunction printers in the International Technology Community (iTC) with CCRA approval.

The IT Security Certification Center participates in the establishment of cPP through the activities of the CCRA Committee, CC Users Forum (CCUF), and the international technical community. Since 2012, it has played the role of the CCMB co-chairs jointly with Germany which is the CCRA subcommittee responsible for developing and revising the CC. By doing so, it has further strengthened the right to speak within the CCRA.

Also, the IT Security Certification Center is a certification organization for the issuing country of the revised CCRA agreement and participates as a reviewing bureau in regular review of CCRA member states. It served as the auditor of the regular audit of the Turkish certification organization in 2014 and the auditor of the regular audit of the Japanese certification organization in 2015. In 2016, it served as the deputy auditor of the periodic review of the Australian certification organization.

Chapter 2

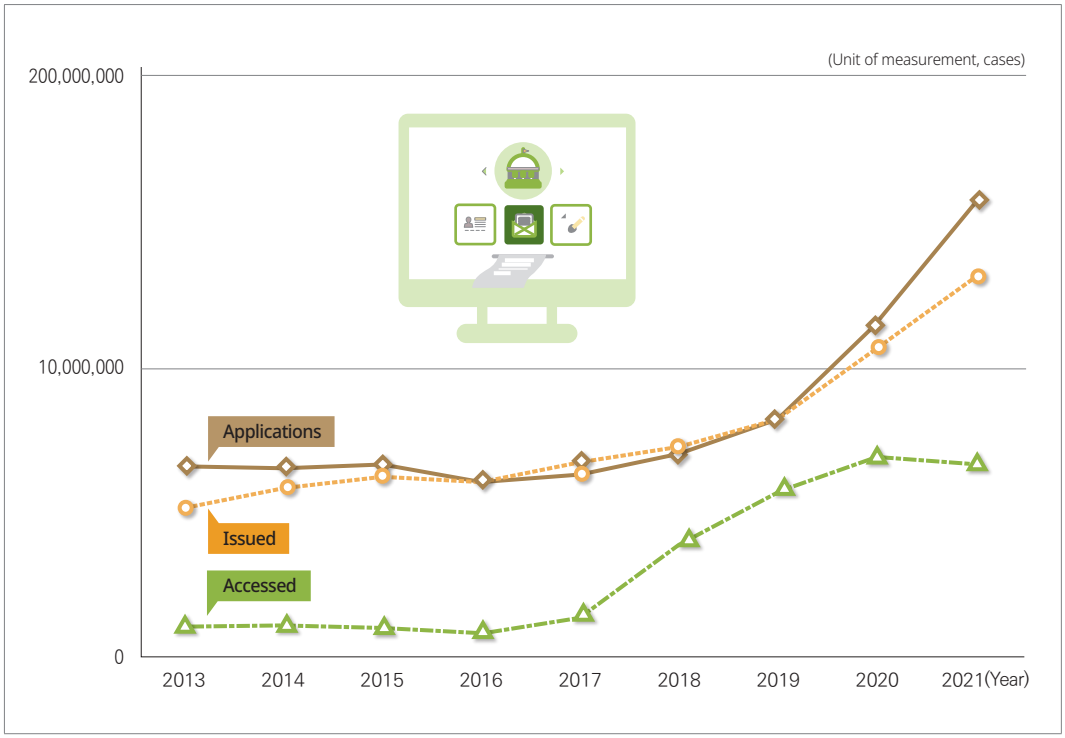
Digital Government

Section 1 Cybersecurity for Digital Government

1. Overview

The rapid development of IT and increased internet usage in the 1990s accelerated the growth of digital government throughout the world. In line with this trend, Korea also opened a one-stop e-government service (G4C) in November 2002, opening the era of e-government in earnest. 'Government 24', a government civil petition portal opened in 2017 after 'Minwon 24' in 2010, has significantly increased the number of service requests from 1.4 million in 2002 to 158 million in 2021. As of December 2021, about 3,600 types of civil complaint applications, browsing, and issuance services are provided online. This shows that 'Government 24' has established itself as a symbolic e-government service that allows citizens to handle civil complaints online without visiting government offices.

Figure 2-2-1-1 'GOV.KR' civil service cases



[Source: The Ministry of Public Administration and Security (Government Civil Service Portal, Government 24, www.gov.kr)]

As Korea strives to develop e-government service with the enforcement of the 「Electronic Government Act」 in 2002, Korea records the top ranks in United Nations' E-government Development Index three times in a row for 2010, 2012, and 2014, also ranked as the top in E-participation Index for 2010, 2012, 2014, 2018 and 2020, and maintain top ranks in ITU's ICT Development Index for 9 years from 2009 to 2017. In addition, Korea ranked first overall in the digital government evaluation conducted for the first time by the Organization for Economic Cooperation and Development (OECD) in 2020. Korea is now offering a wide range of services to the public in areas of tax, trade, tender, civil services, and others through the contribution of continued effort for the service development.

Table 2-2-1-1 Rankings of Korea by International Digitalization Index

(Unit of measurement: ranking (number of nations))

[Organization] Index	Description	Korea ranking (Number of countries surveyed)														
		2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
[ITU] ICT Development Index	Comprehensive evaluation of accessibility, utilization, and utilization capacity of ICT by country	-	-	2(159)	1(159)	1(152)	1(155)	1(157)	2(166)	1(167)	1(175)	2(176)	-	-	-	-
[UN] E-Government Development Index	Competency and willingness to use e-government for ICT-led development by country	-	6(192)	-	1(192)	-	1(193)	-	1(193)	-	3(193)	-	3(193)	-	2(193)	-
[UN] E-Participation Index	Level at which citizens can participate in public policy decision-making online by country	-	2(192)	-	1(192)	-	1(193)	-	1(193)	1	4(193)	-	1(193)	-	1(193)	-
Network Readiness Index	Measurement of the extent to which ICT is used for economic development and competitiveness enhancement by country	19(122)	9(127)	11(134)	15(133)	10(138)	12(142)	11(144)	10(148)	12(143)	13(139)	-	-	17(121)	14(134)	12(130)
[ITU] Global Cybersecurity Index	Comprehensive assessment on 5 cybersecurity pillars by country	-	-	-	-	-	-	-	-	5(193)	-	13(193)	-	15(194)	-	4(194)

※ ICT Development Index: ITU, Measuring the information Society(2018), (ICT Development Index(IDI) This index has not been announced since 2018 as it is in discussions with member countries regarding a revision of the evaluation criteria.)

※ E-government Development Index/E-Participation Index (Biennial announcement): UN, United Nations E-Government Survey (2020).

※ Network Readiness Index: Portulans Institute, The Network Readiness Index (2020).

※ Global Cybersecurity Index: ITU, Global Cybersecurity Index 2021.

In addition to the accomplishment of e-government achieved so far, Korea is recently pursuing digital government innovation to become a leading country in digital government services in the face of rapid change of digital transformation. To this end, promoting the convenient and safe use of digital government services has become a more important task than ever. Korea is promoting the strengthening of government agencies' cybers safety response systems, enhancement of cybersecurity technology, and reinforcement of information security personnel.

2. Main content

The Ministry of Interior and Safety (MOIS) added applicable provisions into the 「Electronic Government Act」, enacted in 2001, to strengthen national cybersecurity governance and infrastructures for diverse digitalization programs, followed by setting up and enforcing government guides as a recommendation. In December 2001, the MOIS appointed high-speed government networks and local administrative networks used by central and local governments as critical information and communications infrastructure and has conducted vulnerability analysis and assessment since April 2002 to establish managerial, physical, and technical protection measures.

To strengthen the security of digital government services to the public, the evaluation index of 'cybersecurity level of digital government service to the public' is being operated according to the plan for performance management and self-evaluation of central administrative agencies. The central administrative agency submits the results of self-evaluation based on detailed indicators to the MOIS, and the MOIS verifies the results and notifies them to each institution, and finalizes the evaluation results after supplementing evidence and making an objection to the results.

To protect the main information systems of central administrative agencies and local governments and the national information and communications network from cyber threats, the MOIS is jointly responding to various cyberattacks through the National Information Resources Agency, the Korea Regional Information Development Institute, and the Cyber Infringement Response Center of metropolitan governments.

The National Information Resources Service (NIRS) intercepts cyberattacks on central governments' systems by monitoring and responding to each type of attack, such as DDoS attacks. The Korea Local Information Research & Development Institute (KLID) operates a computer emergency response team and provides technical support, such as cybersecurity monitoring, and incident response and analysis, to metropolitan cities/provinces and local government systems. Metropolitan governments also operate computer emergency response teams for security monitoring on relevant local governments and affiliated organizations.

In particular, the NIRS established a multi-layer security and defense system such as packet analysis in real-time, blocking a DDoS attack, and cyber shelter

to strengthen its response capability against DDoS for information systems in the national information and communications network. To protect the information system located outside of NIRS with relatively less security infrastructure, the NIRS established additional DDoS defense systems for 300 organizations, including central government-affiliated organizations in 2012, and has been providing defense services since 2013. Furthermore, the NIRS conducts a vulnerability assessment on major information systems at least twice a year and provides technical support by visiting the departments. Vulnerability assessments are also conducted upon requests from each organization to enhance the security of web servers from cyber intrusion attempts. Besides, it prepares for major cyberattacks such as large-scale DDoS and regularly conducts joint cyber response drills with related organizations.

By the 「Act on the Protection of Information and Communications Infrastructure」, the government has designated each ministry's major system as the Critical Information Infrastructure (CII) (424 systems as of December 2021). As the dependence on information and communications services is increasing, the cyberattack on critical infrastructures is also increasing (e.g., cyberattack on an Iranian oil company in 2012, 3.20 cyberterrorism in Korea in 2013).

Accordingly, the MOIS has designated and managed important systems in its jurisdiction as CII (103 systems as of December 2021). To protect CII from cyber threats, it has supported vulnerability analysis and assessment and the establishment of measures and compliance, and supervised the distribution of technical guides. In 2020, the MOIS conducted vulnerability analysis and assessment on eight CII, provided measures for each vulnerability, and took immediate steps to prevent damage from cyberattacks by conducting an emergency security assessment.

Table 2-2-1-2 Critical Information Infrastructures (CII) designated by MOIS

Control System (51)						Information System (52)			Total
Railway operation	Traffic signal	Water supply	District heating	Smart City	Water reclamation	Emergencyrescue	City/province administration	MOIS	103
13	12	16	2	5	3	19	17	16	

Along with this, the MOIS has set up Information Sharing and Analysis Center (ISAC) for local governments at KLID since February 2013. Besides, the MOIS has conducted

vulnerability analysis and assessment for each metropolitan local government - internet and internal system, traffic signal control system, railroad control system, and water purification control system, and supported setting up a protection plan.

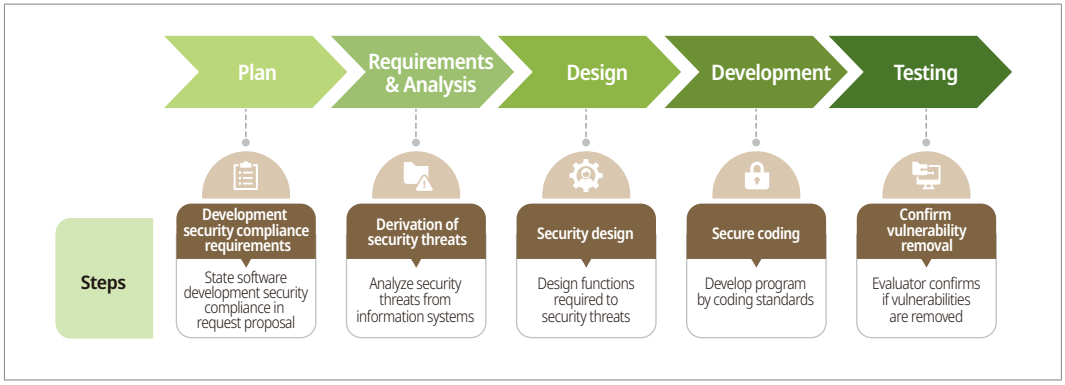
Section 2 Software Development Security

1. Overview

The recent increase of cyberattacks exploits software vulnerabilities before security patches such as zero-day attacks and website hacking. In particular, more than 75% of cyberattacks exploit application's vulnerability, which highlights the need and importance of detecting and removing vulnerabilities at the software development stage.

'Software Life cycle model' is to develop secure software that can respond to security incidents by reducing software embedded vulnerabilities caused by mistakes by the developer and logical errors in the software development process.

Figure 2-2-2-1 Software life cycle model



In 2012, the MOIS revised and announced the 「Guide to the implementation/ operation of information systems for administrative agencies and public institutions」. The guide is to provide security standards and procedures for secure software development so that administrative agencies and public institutions comply with them. Based on the size of the digitalization project, it gradually expanded the obligation to

comply with the secure software development to projects with 4+ billion KRW in 2013, 2+ billion KRW in 2014, and all entities for supervision in 2015.

In 2016, the MOIS strengthened the security of the information system by expanding the scope of software development security from the implementation stage to the design stage when promoting the information system. And, in 2018, the MOIS provided a basis for the estimate of security-enhanced development to calculate the cost for the adoption of software security-enhanced development, by amending the 'Software Cost Estimation Guidelines'.

Table 2-2-2-1 Overview of secure software development processes

	Content	Remark
Grounds	• Articles 50~54 of Guide to the implementation/operation of information systems for administrative agencies and public institutions • Article 26 of Guideline for Management of Mobile e-Government Service	Electronic Government Act
Object	• Digitalization project for information system supervision ※ 4 billion KRW or more (2013. 1.) → 2 billion KRW or more (2014. 1.) → All supervision targets (2015. 1.) • Mobile e-government service (2014.9, all mobile e-government services) ※ Mobile web, mobile apps, hybrid apps, etc.	Escalation
Scope	• Output and all source code in the design phase(all new development, parts changed due to maintenance)	Excluding commercial software
Standard	• Security design criteria at software design phase(Guideline Attached Table 3, 20 items including DBMS inquiry and result verification)	Software security vulnerability (design phase)
	• Criteria for removing security vulnerabilities in software development phase(Guideline Attached Table 3, 49 items including SQL insertion)	Software security vulnerability (development phase)
	• Standards for checking security vulnerabilities in mobile apps(Guideline Attached Table 3, 26 items including SQL insertion)	Mobile security vulnerability
	• Standards for checking security vulnerabilities in mobile apps(Guideline Attached Table 1, 20 items including errors during repeated installation)	Mobile security vulnerability

Criteria for software vulnerability have 20 items in the design phase, and 49 in the implementation phase. In 2012, 43 vulnerabilities were established in the implementation phase, and the number was expanded to 47 in 2013, and further expanded to 49 in 2020 to respond to the latest security threats. To be applied for development security from the software designing phase, 20 items were newly included for security design criteria in 2016 and regulated its scope to apply to start from the design output.

As the use of mobile e-government services has increased, the need for development security for mobile services has increased. Accordingly, the MOIS revised the 「Guideline for Management of Mobile e-Government Service」 in 2014 (an established rule of the MOIS) to find and fix security vulnerabilities of mobile e-government services, and established 26 vulnerability assessment criteria specialized in mobile e-government services.

2. Foundation for digital government

For secure software development to be a fixed and well-grounded culture, the government conducts vulnerability assessments on e-government software and security validation on mobile e-government services since 2009. Also, to raise awareness of secure software development, the government carries out various activities such as distributing security guides, providing education, operating a qualification system, and holding contests.

A. Vulnerability assessment on e-government software

From 2009 to 2012, the government supported the vulnerability assessment on source codes and remedial measures for newly developing information systems in administrative/public agencies. Since 2013, the scope for assessment has expanded to the systems in operation.

Table 2-2-2-2 Assessed units for software vulnerability

(Unit of measurement; cases)

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
No. of verifications	2	10	23	33	161	31	35	60	87	91	99	127	80

B. Security verification for mobile e-government service apps

The KISA opened the 'e-Government Mobile App Security Verification Center', to improve the security and reliability of mobile e-government service apps in 2011, performed security verification on 850 mobile apps by 2014, and continued its support through the 'e-government software and IoT security center'.

Table 2-2-2-3 Security verification on mobile e-government apps

(Unit of measurement; cases)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
No. of verifications	30	240	286	292	345	218	366	158	171	187	208	2,501

C. Secure software development guide

The MOIS has developed and released a guideline for secure software development to suggest a safe development method that fixes security vulnerabilities when developing software. It is distributing a total of 9 volumes, including six secure software development guides and three mobile-related guides, and constantly revising them according to changes in the software development system and security vulnerability criteria. In 2019, three volumes were amended and released: 'guide for secure software development', 'guide for software vulnerability assessment', and 'guide for development security assessment using open software'.

Table 2-2-2-4 The guideline of secure software development

Guide	Released	Latest Version	Content
Guide for secure software development	June, 2011	November, 2021	Description of procedures and methods for applying secure software development
Java secure coding guide	June, 2011	September, 2012	Providing security vulnerabilities and coding examples specialized in Java development language
C secure coding guide	June, 2011	September, 2012	Providing security vulnerabilities and coding examples specialized in C development language
Mobile app source code verification guidelines	August, 2011	October, 2021	Description of how to apply for security verification of mobile e-government service apps
Android-Java secure coding guide	September, 2011	September, 2011	Providing security vulnerabilities and coding examples specialized in Android-Java development language
Guide for software vulnerability assessment	May, 2012	November, 2021	Description of diagnostic methods and countermeasures for software security vulnerabilities
Guide to building mobile public service	October, 2014	December, 2015	Provision of items to be considered when establishing and operating a mobile public service
Mobile public service security vulnerability inspection guide	October, 2014	December, 2015	Providing assessment procedures and methods for 20 mobile app vulnerability criteria
Guide for Development Security assessment using open software open software	February, 2016	June, 2019	Executive Summary of development security assessment methods using diagnostic tools

D. Awareness campaigns

To raise awareness of secure software development, education on secure software development methodology to find and fix the vulnerabilities in the development phase is conducting for government officers, developers, and supervisors since 2009. Since 2012, a vulnerability assessment training course has been opened to produce experts, and 622 expert trainees have been produced by 2021.

Table 2-2-2-5 Education on secure software development

(Unit of measurement; persons)

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
Education on secure development	109	266	1,019	2,262	2,544	2,100	1,432	1,588	1,866	2,335	1,590	1,313	1,740	20,059
Vulnerability assessment expert qualification	-	-	-	82	143	120	111	41	25	28	17	23	32	622

Besides, since 2011, secure software development conferences have been held annually for government officers, developers, and vulnerability assessment experts to share the results of secure software development systems and have a discussion for improvement. Since 2014, contests for university students, who are future software developers, have been held to promote and stimulate interest in secure software development.

Section 3 **Digital Signature**

1. Digital Signature Certificates for Government

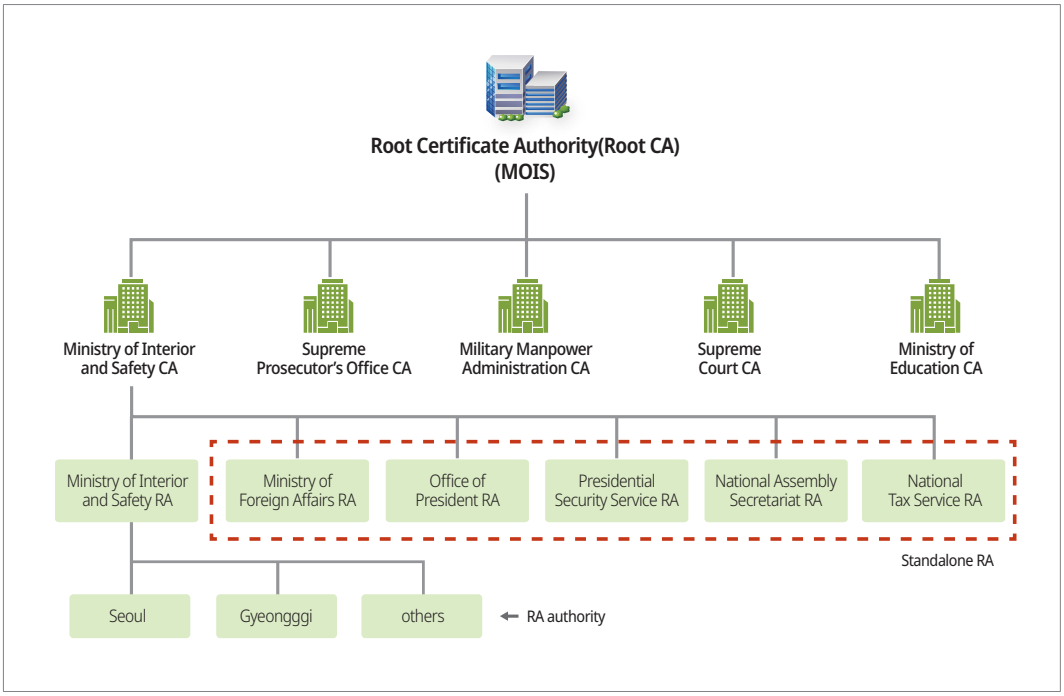
A. Overview

As the working environment of digital government has been changed from paper-based to electronic document, potential loss including exposure, alteration, and damage to key information by hacking has also increased, therefore, the countermeasures are explored to ensure the distribution continuity and safe recovery of electronic documents. The government therefore established and operated the Government Public Key Infrastructure (GPKI) for stable distribution of electronic documents, identification of public officers of administrative/public agencies on transmission and reception of electronic documents, and prevention of forgery/alteration.

The GPKI is operated in accordance with article 29 of the 「Electronic Government Act」 and article 28 of the Enforcement Decree of the same Act. The GPKI became the authentication system for e-government by implementing the system and interconnecting private and public digital signatures in December 2002. An escrow/recovery management system for encryption keys was established in February 2006 to ensure continuity and stability of the administrative tasks. The public and financial certification system was established in 2006 to expand and distribute the GPKI to public and financial institutions as well. To assure reliability and trust of the certificate for government digital signature, the GPKI system was upgraded by upward adjustment on signature key length (2,048 bits) and replacing hash algorithms in 2011.

In 2012, the GPKI improved its software so that it could be issued and used in various web browsers. Also, the GPKI completed system upgrade for stable service in 2014, and in 2015, it became the first domestic certificate authority to acquire WebTrust certifications in the fields of 'WebTrust for Certificate Authority (CA) ' and 'WebTrust for Secure Sockets Layer (SSL)'.

Figure 2-2-3-1 Government Public Key Certification Scheme



The GPKI consist of the Root Certificate Authority (Root CA), which is the MOIS, 5 accredited CAs designated by the director of MOIS, and 974 registration authorities (RA) designated by each CA. The GPKI provides user authentication by mutual compatibility with the National Public Key Infrastructure (NPKI).

Table 2-2-3-1 GPKI Certificate Authorities (CA)

(Unit of measurement: place)

	Number of authorities	Designated authorities
Root CA	1	• Ministry of Interior and Safety
CA	5	• Ministry of Interior and Safety, Ministry of Education, Supreme Prosecutor's Office, Military Manpower Administration, Supreme Court (National Court Administration)
RA(including sub-authorities)	974	• Central administrative agency: 64 institutions including the Executive Office of the President • Local governments: 17 institutions including Seoul Metropolitan Government • Organizations and committees affiliated with each agency

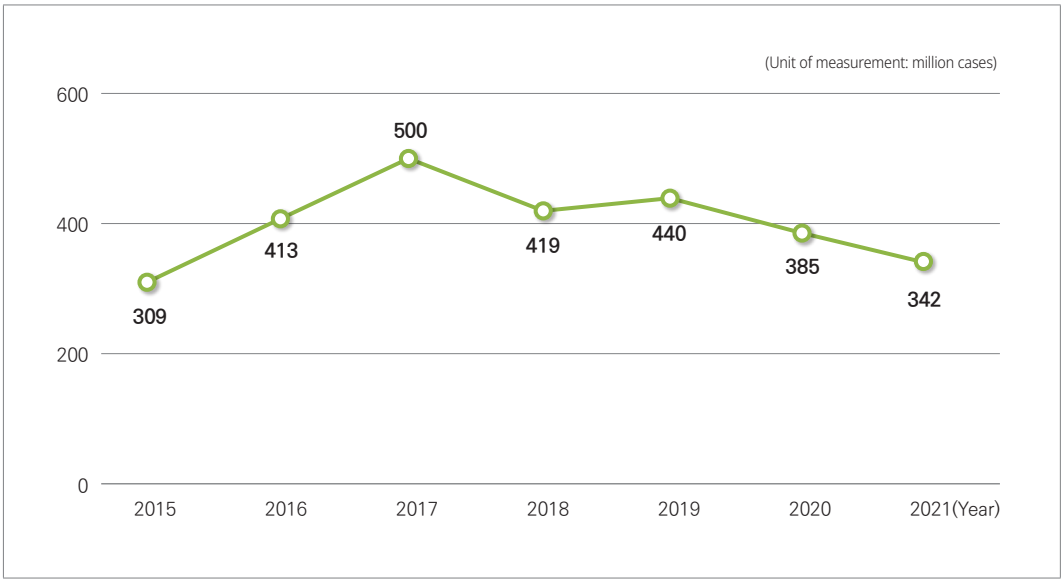
Table 2-2-3-2 **Roles of different authorities in GPKI**

	Role
Root CA	• Designate accredited CAs, Certificate Issue for CAs • Establish GPKI technical standard and mutual compatibility with NPKI • Create a CAs' facility and device standard and survey on the management of CAs • Post a certificate and certificate revocation list
CA	• Construct the authentication system complying with technical standard • Designate and manage RAs, identify user authentication
RA	• Receive authentication applications, identify and register user authentication • Designate and manage Local RAs(LRA)

B. Certificate issue and usage

As of December 2021, 7.21 million GPKI certificates have been issued for the identification of government officers and preventing forgery of electronic documents, and are used in 11,067 administrative services by 1,493 organizations. For privacy protection, the government supports setting up a secure server by deploying Government Secure Socket Layer (G-SSL) certificates to those websites.

Figure 2-2-3-2 **GPKI certificates usage**



C. Authentication service expansion

In order to enhance the stability of the e-government services against external threats with ever-evolving hacking techniques, the government provides various authentication services such as government One Time Password (OTP), multi-factor authentication (2 channels), and electronic document authenticity verification.

In 2015, the GPKI has reached its limit to maintain trust only by independent agreements, due to technological changes and browser policy changes. Accordingly, the government promoted multiple international certification schemes to acquire managerial/technical trust in the GPKI. In October 2015, for the first time among domestic certification agencies, it acquired WebTrust certifications in the fields of 'WebTrust for CA' and 'WebTrust for SSL'. It also joined the CA/Browser Forum to participate in international standardization.

2. National Digital Signature Scheme

A. Overview

In February 1999, the government enacted the 「Digital Signature Act」, which established fundamentals on digital signature, to ensure the safety and reliability of electronic documents and promote their use.

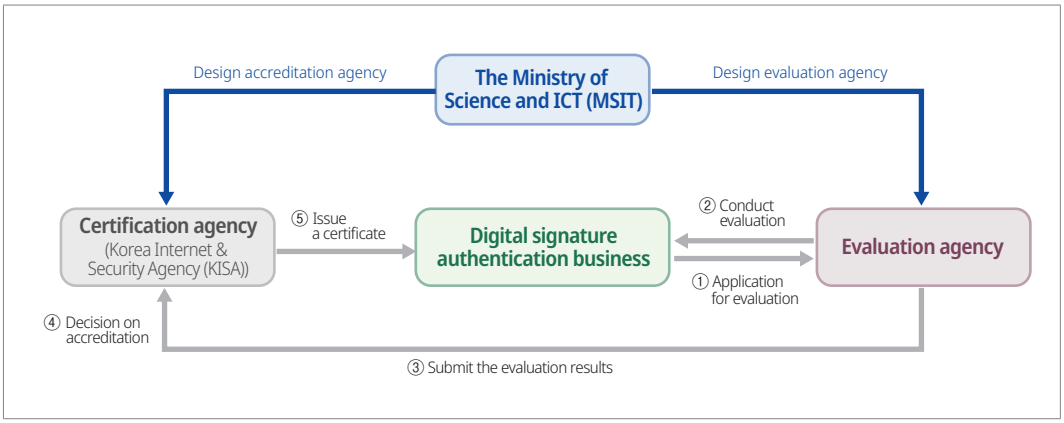
The NPKI were widely used in the early days of the introduction of the electronic signature system in Korea, contributing greatly to national informatization promotion such as activation of e-commerce. However, it also raised many problems such as causing a market monopoly, hindering the development of digital signature technology and service innovation, and limiting the people's right to choose various and convenient electronic signatures.

In order to solve these problems, the NPKI system was abolished. To create conditions in which various digital signatures can compete without discrimination based on their technologies and services, to enhance the reliability of digital signatures, and to provide the public with a choice of digital signature certification services, a new accreditation and evaluation scheme of digital signature certification service was introduced. The amended 「Digital Signature Act」 came into effect in December 2020.

B. Accreditation and evaluation on digital signature certification service providers

To secure the stability and reliability of the digital signature certification service and to guarantee the people's various and convenient options for digital signatures, a private evaluation agency evaluates whether the digital signature certification service complies with the operating standards. And, the accreditation body decides whether to accredit it or not by reviewing the adequacy of the result.

Figure 2-2-3-3 Accreditation and evaluation of digital signature certification



The Ministry of Science and ICT (MSIT) establishes policies to enhance the safety, reliability, and diversity of digital signatures, and the KISA performs several tasks such as determining whether the applicant has complied with the operational standards for digital signature authentication and withdrawing approval. And, the three private business operators selected as evaluation agencies (December 22, 2020) evaluate whether the digital signature authentication business that applied for the evaluation complies with the operating standards.

Table 2-2-3-3 Selection of evaluation agencies (as of December 2021)

	Evaluation agency	Evaluation results	Date of selection
1	Telecommunications Technology Association	Passed	December 22, 2020
2	Financial Security Institute	Passed	December 22, 2020
3	Deloitte Anjin LLC	Passed	December 22, 2020

C. Accreditations

After the amended 「Digital Signature Act」 came into force, the Korea Internet & Security Agency issued accreditations to 16 digital signature certification service providers.

Table 2-2-3-4 Accreditations Issued

Accreditation number	Company	Scope of Accreditation	Term of validity
2021-001	NHN PAYCO	PAYCO authentication service	August 26, 2021 ~ August 25, 2022
2021-002	Shinhan Bank	Shinhan Sign service	September 15, 2021 ~ September 14, 2022
2021-003	Naver	Naver certificate service based on mobile app	September 17, 2021 ~ September 16, 2022
2021-004	Kookmin Bank	KB Mobile Certificate	October 14, 2021 ~ October 13, 2022
2021-005	Korea Financial Telecommunications & Clearings Institute	YesKey Certificate Service (Joint Certificate and Financial Certificate)	October 21, 2021 ~ October 20, 2022
2021-006	Korea Information Certificate Authority	Joint authentication service	November 4, 2021 ~ November 3, 2022
2021-007	Viva Republica	Toss certificate	November 11, 2021 ~ November 10, 2022
2021-008	Bank Salad	Bank Salad certificate	November 11, 2021 ~ November 10, 2022
2021-009	Kakao	Kakao certificate	November 22, 2021 ~ November 21, 2022
2021-010	Koscom	Koscom SignKorea authentication service	November 22, 2021 ~ November 21, 2022
2021-011	Korea Electronic Certification Authority	Joint Certificate	November 26, 2021 ~ November 25, 2022
2021-012	Korea International Trade Association	TradeSign authentication service (joint certificate)	December 7, 2021 ~ December 6, 2022
2021-013	Hana Bank	Hana OneSign certificate service	December 30, 2021 ~ December 29, 2022
2021-014	SK Telecom	SK Telecom PASS certificate service	December 30, 2021 ~ December 29, 2022
2021-015	KT	KT PASS certificate	December 30, 2021 ~ December 29, 2022
2021-016	Korea Information Certificate Authority	S-PASS certificate service	December 30, 2021 ~ December 29, 2022

D. Digital signature for private sector

The Ministry of Interior and Safety (MOIS) took a preemptive response to the revised Electronic Signature Act. In January 2021, the MOIS deployed a pilot application for digital signatures in private sector such as Kakao and Telecommunication Company Pass, so-called 'Easy Authentication', to major public websites such as Government24 and Hometax so that citizens can conveniently login and use digital government services. As of December 2021, the MOIS completed to apply to 55 public websites such as 'Virtual Assistance Service for the Public', Wetax, and Bokjiro, and plans to continue to expand to public websites by including additionally recognized private digital signatures, such as Naver and Shinhan Bank, in 'Easy Authentication.'

Figure 2-2-3-4 **'Government 24' login screen with Easy Authentication**

In addition, the Ministry of Science and ICT (MSIT) in cooperation with the Korea Centers for Disease Control and Prevention (KCDC) added easy digital signatures such as Naver, Kakao, and PASS, which are commonly used by the public, to the reservation system for COVID-19 vaccine to make it easier and more convenient for COVID-19 vaccination reservation, and plans to continuously expand the easy digital signatures in the future.

In January 2022, the Financial Services Commission (FSC) implemented the MyData service of 'Financial Assistant in My Hand'. MyData in the financial sector helps managing assets and credits, such as collecting and displaying scattered personal credit information in one place and recommending suitable financial products by analyzing the financial status and consumption patterns. Integrated authentication, which simplifies the complex authentication process and allows multiple information providers to request information transmission with only one identity authentication, has been introduced. Private digital signatures that have been linked in accordance with the MyData integrated certification standard after being evaluated and acknowledged for compliance with the operational standards of the digital signature certification business are also being used as a MyData integrated authentication method.

Chapter 3

Critical Information Infrastructure Protection

Section 1 Governance Structure

1. Overview

With the development of the information and communications infrastructure in the 2000s, national infrastructures such as government administration, broadcasting and communication, finance, and energy became more dependent on information and communications technology. As a result, cyberattacks such as hacking, distribution of malicious codes, and DDoS attacks emerged as a new threat. However, while interruption or disruption of critical information and communications infrastructure can cause enormous economic losses and social confusion, the laws and regulations governing the prevention and response systems for electronic infringement activities were insufficient. Accordingly, the 「Act on the Protection of Information and Communications Infrastructure」 was enacted in 2001 to establish a pan-governmental response system to protect the information and communications systems of critical infrastructure from cyberattacks such as hacking and malicious code.

In 2007, reflecting the changes in the ICT environment and the current system's deficiencies, the Working Committee under the Committee for Protection of

Information and Communications Infrastructure was divided into public and private sectors to clarify its role. In addition, the heads of state agencies prescribed by the Presidential Decree, such as the Director of the National Intelligence Service (NIS) and the Minister of Science and ICT (MSIT), recommended the designation of critical information and communications infrastructure to the central administrative agency and gave the authority to verify the implementation of measures to protect critical information and communications infrastructure.

In 2009, the 「Information and Communications Technology Industry Promotion Act」 was enacted to promote effective information and communications industry promotion policies. Accordingly, the provision of information protection consulting specialists in the 「Act on the Protection of Information and Communications Infrastructure」 was transferred and changed to a knowledge information security consulting specialist under the 「Act on the Protection of Information and Communications Infrastructure」. In 2015, as the 「Act on the Promotion of Information Security Industry」 was promulgated, a knowledge information security consulting specialist was changed to an information security professional service company.

The revised enforcement decree in 2012 reflected matters mandated by the revision of the 「Act on the Protection of Information and Communications Infrastructure」 in December 2007 and clarified a more specific composition and operation method in line with the changes of the Working Committee. Also, it included matters related to the report on the implementation of the protection measures by the director of the NIS and the recommended method for designating critical information and communications infrastructure. Furthermore, some deficiencies in the operation were improved and supplemented, such as shortening the vulnerability analysis and evaluation cycle from two years to one year. Also, systematic improvements were made by expanding the scope of support organizations to protect critical information and communications infrastructure.

In 2015, with the government having established and operated the Information Sharing & Analysis Center (ISAC) to jointly analyze cyber threats between infrastructure management agencies in the same industry and to promote information sharing, the grounds were prepared for the government to provide financial as well as technical support. Moreover, it laid the groundwork for encouraging new establishments by simplifying procedures such as removing the

notification obligation when establishing ISAC.

The effectiveness of the designation recommendation system introduced to effectively protect critical information and communications infrastructure by explicitly stipulating matters on the designation and cancelling designation of critical information and communications infrastructure in the deliberations of the Committee for Protection of Information and Communications Infrastructure and the Working Committee in 2018 was secured.

Some deficiencies in the operation of the current system were improved and supplemented in 2019 when necessary to protect critical information and communications infrastructure from new forms of cyberattacks, or when a separate vulnerability assessment is necessary due to significant changes in critical information and communications infrastructures, such as establishing a legal basis for the head of the central administrative agency to order the head of the relevant management agency to analyze and evaluate the vulnerability of critical information and communications infrastructure.

New vulnerability analysis and evaluation items according to changes in the ICT environment in 2021 were reorganized jointly by the MSIT and the NIS (2019-2021) and announced in March 2021. Besides, the ability to respond to cyberattacks on major information and communications infrastructure was further strengthened. Furthermore, for the efficient management of critical information and communication infrastructure, the Enforcement Decree of the 「Act on the Protection of Information and Communications Infrastructure」was amended. With the amendment, the legal basis for the deadline for notification of the designation result after the designation decision (within 30 days) and the deadline for implementation (within six months) was established.

2. Promotion system

For the stable management and operation of critical information and communications infrastructure, the government is making efforts to prevent and respond to cyberattacks between related central administrative agencies to cooperate and complement each other, by operating the Committee for Protection of Information and Communication Infrastructure and directing and coordinating the establishment and implementation of information and communications infrastructure protection policies.

The Committee for Protection of Information and Communications Infrastructure is composed of the Minister for Government Policy Coordination as its chair and the vice- minister-level public officials of the central administrative agency as members. The Committee for Protection of Information and Communications Infrastructure deliberates on major policy matters, such as adjustment of protection policies for critical information and communications infrastructure, synthesis and adjustment of protection plans for critical information and communications infrastructure, improvement of systems related to the protection of critical information and communications infrastructure, and new designation and cancelling designation of infrastructure.

Moreover, there is a Working Committee for Protection of Information and Communications Infrastructure established to efficiently operate and support the Committee for Protection of Information and Communications Infrastructure. The Working Committee reviews and deliberates on the agenda submitted to the Committee for Protection of Information and Communications Infrastructure and the matters delegated by the Committee for Protection of Information and Communications Infrastructure or directed by a Chairperson of the Committee for Protection of Information and Communications Infrastructure.

The Working Committee operates the Public Sector Working Committee (Chair: Deputy Chief of the NIS) and the Private Sector Working Committee (Chair: Vice Minister of the MSIT). Moreover, the Working Committee distributes protection measures and guidelines for establishing protection plans and plays a role in recommending new designation of critical information and communications infrastructure.

Meanwhile, the central administrative agency establishes and implements a protection plan after designating critical information and communications infrastructure and reviewing measures to protect critical information and communications infrastructure submitted by the management agency. In order to prevent and respond to infringement incidents on critical information and communications infrastructure, the management agency conducts vulnerability analysis and evaluation of the relevant facilities and prepares protection measures. And, in the event of an accident, the relevant central administrative agency and investigative agency are notified of the accident and promptly carry out restoration work.

In particular, in the event of a widespread serious breach of critical information and communications infrastructure, the Headquarters for Countermeasures against Intrusion Information and Communications Infrastructure under the Committee for Protection of Information and Communications Infrastructure is temporarily operated to perform emergency response, technical support, and damage recovery.

Supporting organizations to protect critical information and communications infrastructure include the Korea Internet & Security Agency (KISA), National Security Research Institute (NSR), the Information Sharing & Analysis Center (ISAC), and enterprises specializing in information security services. These support organizations provide technical support for establishing measures to protect critical information and communications infrastructure and preventing and recovering from cyberattacks.

Figure 2-3-1-1 Promotion system for protection of critical information and communications infrastructure

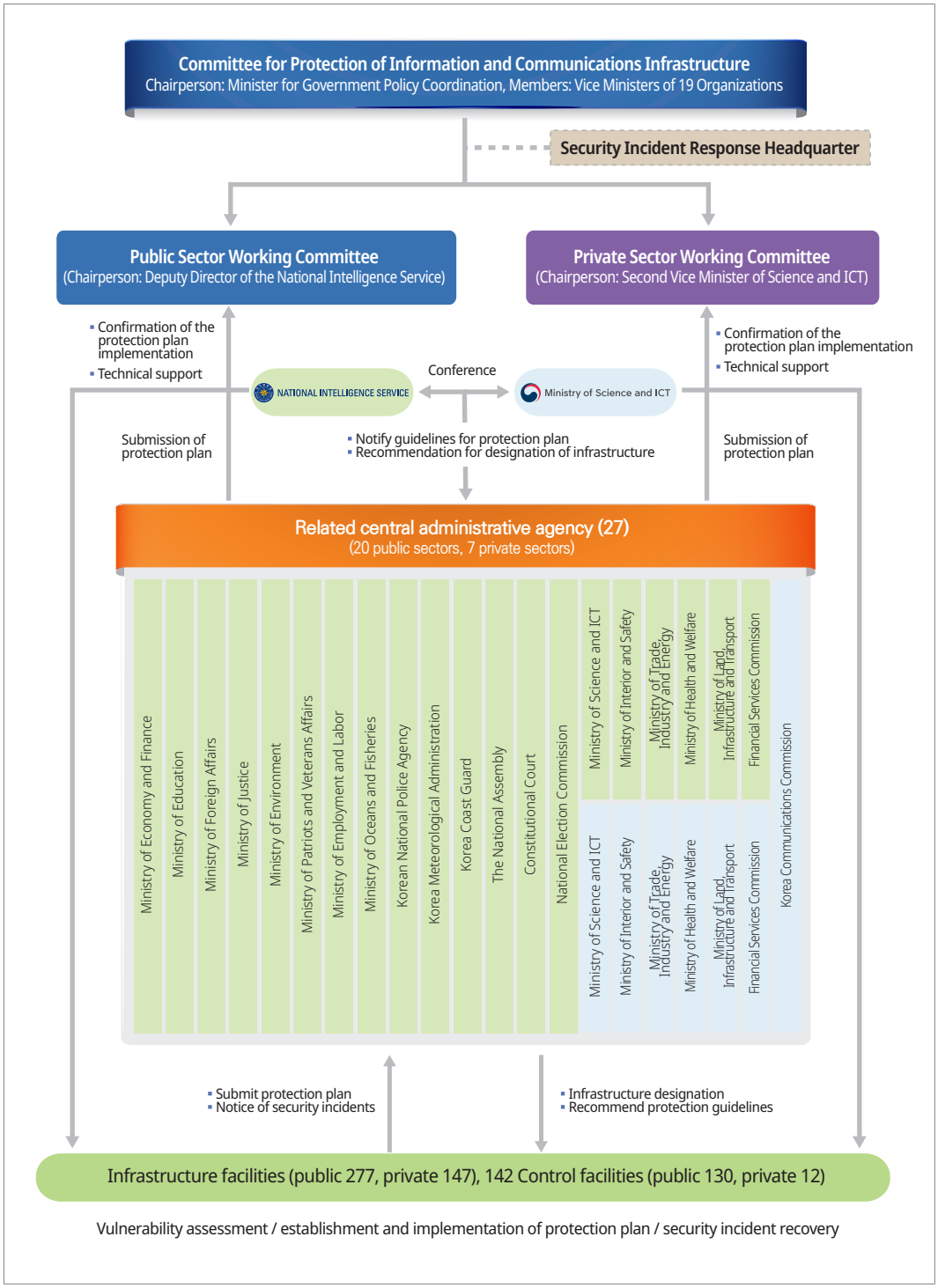


Table 2-3-1-1 Main functions by performing subject

Execution subject	Main function
Committee for Protection of Information and Communications Infrastructure (Office for Government Policy Coordination)	• Infrastructure protection policy and deliberation of system improvement • Operation of security incidents countermeasure headquarters
Central administrative agency	• Establishment of protection plan in the area under jurisdiction and enactment and revision of protection guidelines • Order and recommendation of protective measures for management institutions • New designation and cancelling designation of Critical Information Infrastructure (CII)
Management Institution	• Establishment of protection analysis and evaluation of vulnerability assessment of facilities under jurisdiction • Self-evaluation of new designation and cancelling designation of infrastructure • Notification of security incidents and recovery
NIS / MSIT	• Preparation and distribution of guidelines for establishing protection and plans • Confirmation of implementation of protection measures by management agency and technical support • Establishment and revision of criteria of vulnerability assessment
KISA / NSR / ISAC / Enterprises specializing in information security services	• The analysis and evaluation of vulnerability • Prevention and recovery support for security incidents • Ascertaining implementation of measurement to protection critical information and communication infrastructure

Section 2 Main Activities

1. Designation and cancelling designation of critical information and communications infrastructure

Regarding the designation and cancellation of designation of critical information and communications infrastructure, the head of each central administrative agency designates information and communications infrastructure that is deemed necessary to protect against digital infringement. The head may cancel the designation when the designation can no longer be maintained due to the disposal, consolidation, or business

transfer of the relevant facility. In addition, in the case of designation or cancellation of designation, it shall undergo deliberation by the Committee for Protection of Information and Communications Infrastructure, and the result shall be announced.

Table 2-3-2-1 Criteria for designation of critical information and communications infrastructure

① The national and social importance of the work performed by the organization managing the relevant information and communication infrastructure
② The inter-connection with other information and communications infrastructure
③ Interconnection with other information and communications infrastructure
④ The areas and extent of damage caused by intrusion incidents to the national security, economy and society, if any
⑤ The probability of intrusion and the easiness of restoration

The subject of designation of critical information and communications infrastructure includes not only state and public institutions but also information and communications infrastructure operated and managed by the private sector. Furthermore, when a security incident occurs, it includes electronic control and operation systems and information and communications networks related to national security, government administration, defense, public order, finance, broadcasting, communication, transportation, energy, etc. that can have a significant impact on the lives and economic stability of the people.

Moreover, the MSIT and the NIS may recommend the designation of critical information and communications infrastructure to each central administrative agency. The head of a central administrative agency who has received a recommendation that the infrastructure under his jurisdiction needs to be designated as a critical information and communications infrastructure undergoes deliberation by the Committee for Protection of Information and Communications Infrastructure on whether to designate the relevant facility in accordance with the「Act on the Protection of Information and Communications Infrastructure」. After that, according to the amended Enforcement Decree of the 「Act on the Protection of Information and Communications Infrastructure」 (March 2021), the result shall be notified to the Minister of Science and ICT and the Director of the NIS within 30 days.

As of December 2021, a total of 424 types of critical information and communications infrastructure, including 139 management agencies and 277 facilities in the public

sector, 90 management agencies, and 147 facilities in the private sector, are being designated and managed.

Figure 2-3-2-1 Procedure for designating critical information and communications infrastructure

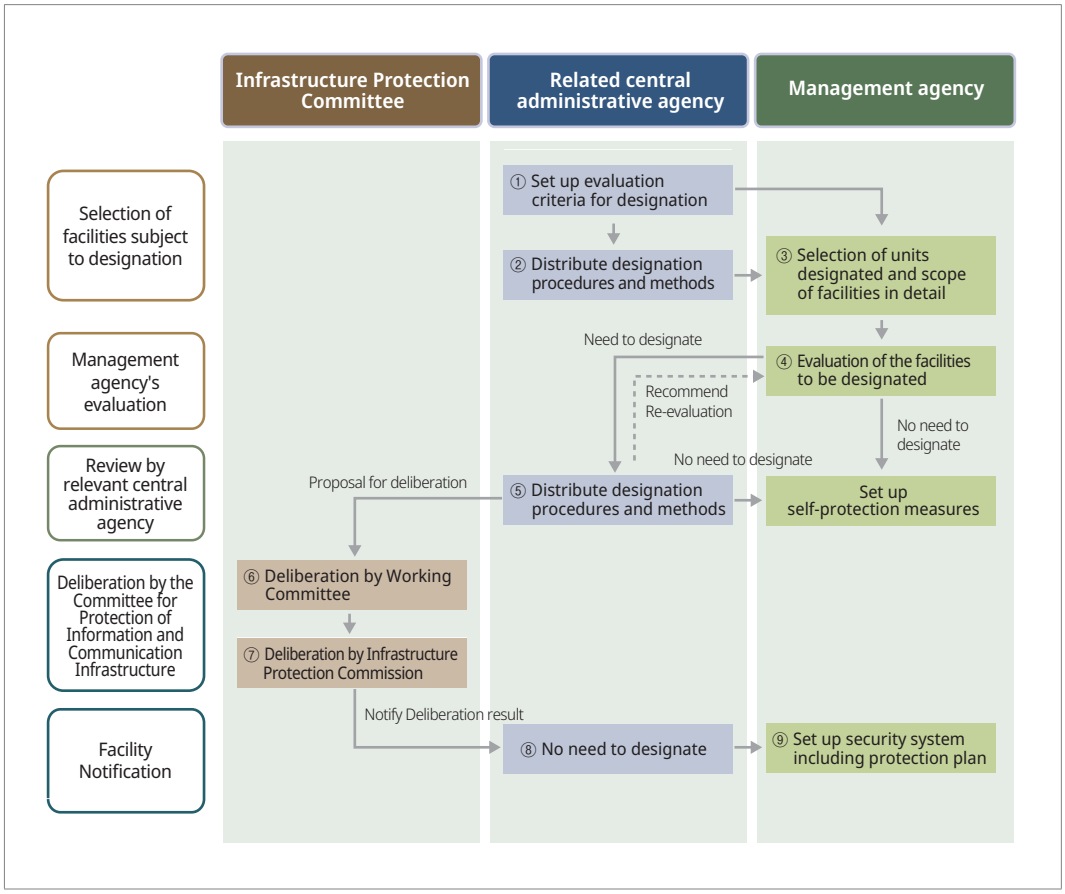


Figure 2-3-2-2 Procedure of recommendation for designation of critical information and communications infrastructure

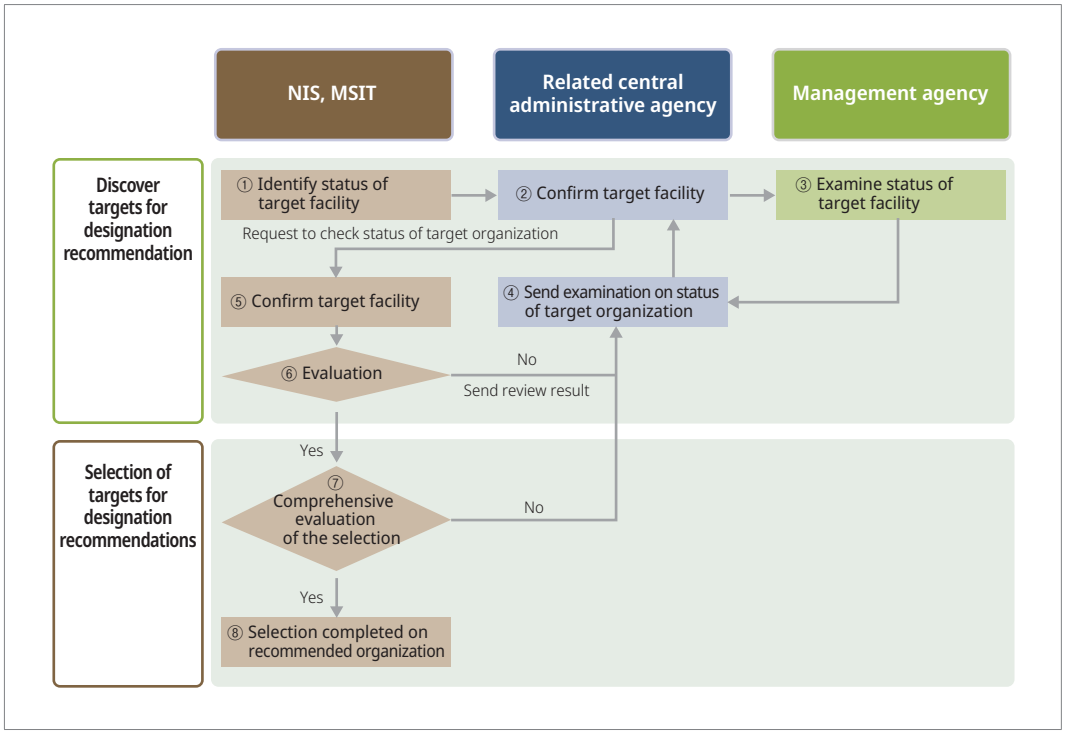


Table 2-3-2-2 Designation status of critical information and communications infrastructures

	2012	2013	2014	1015	2016	2017	2018	2019	2020	2021
Public	114	135	193	227	243	252	262	265	274	277
Private	72	74	99	127	142	141	149	149	148	147
Total	186	209	292	354	385	393	411	414	422	424

The head of the relevant central administrative agency may cancel the designation of critical information and communications infrastructure ex officio or upon request of the relevant management agency if the management agency abolishes, suspends, or changes its business. The designation of critical information and communications infrastructure of an institution managed and supervised by the head of a local government may be revoked by the Minister of Interior and Safety (MOIS) in consultation with the head of the local government. Meanwhile, if the head of the central administrative agency wishes to cancel the designation of critical information

and communications infrastructure, it must undergo deliberation by the Committee for Protection of Information and Communications Infrastructure.

2. Vulnerability analysis and evaluation

The head of the management agency shall establish protection measures for critical information and communications infrastructure every year. Through this, the head of the management agency discovers and removes new vulnerabilities in the short term, and establishes an effective management system in the long term by analyzing the impact of security incidents.

Besides, in accordance with the Enforcement Decree of the 「Act on the Protection of Information and Communications Infrastructure」 (March 2021), the head of the management agency must conduct vulnerability assessments within 6 months when critical information and communications infrastructure is newly designated. However, if there is a particular reason for not performing the vulnerability assessments for the facility within 6 months after the designation of the relevant critical information and communications infrastructure, it must be carried out within 9 months of designation after obtaining approval from the competent authority.

The analysis and evaluation of vulnerability were previously conducted every two years, but the need for shortening this period was raised in consideration of increasing number of new cyber threats each year. Accordingly, through the revision of the 「Enforcement Decree of the Information and Communication Infrastructure Protection Act」 in 2012, the analysis and evaluation of vulnerability should be conducted once a year. Furthermore, if a significant change has occurred in the main information and communications infrastructure under the jurisdiction or if the management agency determines that it is necessary, the assessments of the vulnerability may be carried out even when less than one year has passed.

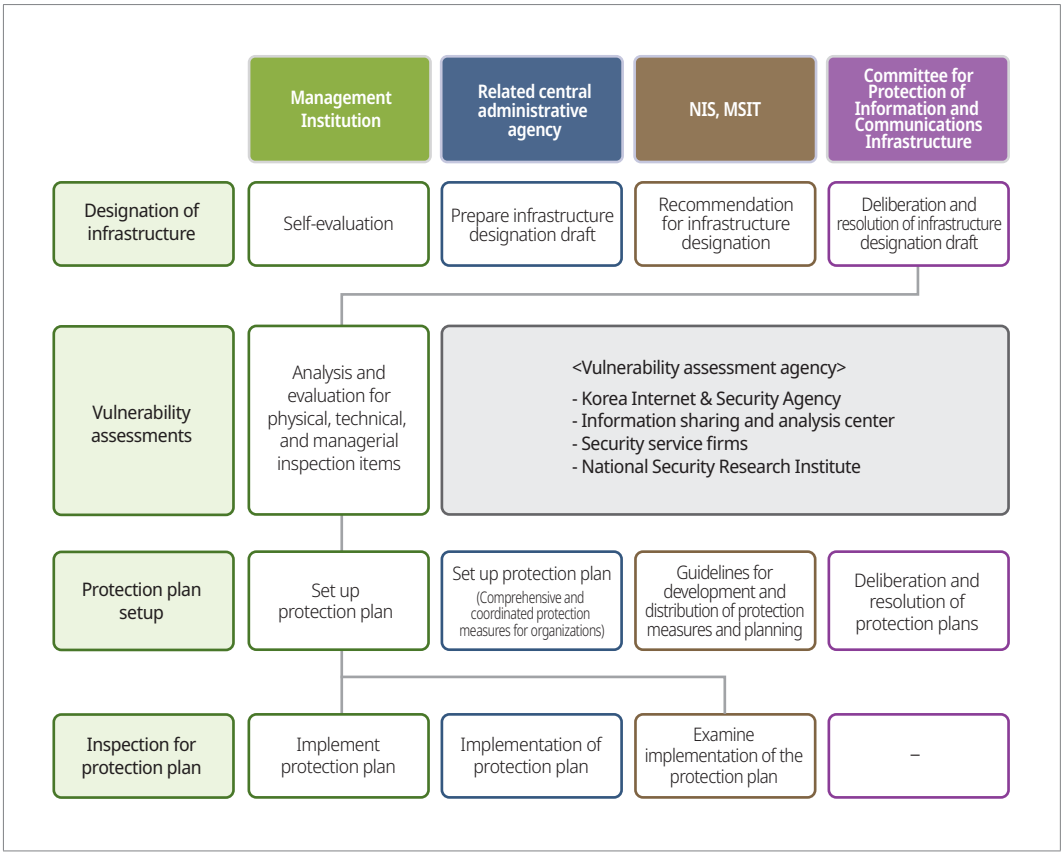
In accordance with Article 9 of the 「Act on the Protection of Information and Communications Infrastructure」, the head of the management agency may form an internal task force for vulnerability assessments to perform these tasks on the facilities in charge or entrust it to the KISA, NSR, ISAC, and enterprises specializing in information security services.

The MSIT and the NIS revised the 「Vulnerability Analysis/Evaluation Criteria for Critical Information and Communication Infrastructure」 (The Ministry of Science and ICT Notification No. 2021-28) to prepare for the changing cyber threats, by creating new items for security management such as account management of cloud systems and deleted similar or duplicate items from the existing. The new criteria have established the definition of vulnerabilities that cannot be handled which cannot be improved and need special care, so that the management agencies are required supplementary measures. Regarding this issue, the MSIT published a detailed guide on how to analyze and evaluate technical weaknesses of critical information and communications infrastructures (March 2021) to support management agencies, and distributed to the Bohonara (www.boho.or.kr) managed by the KISA.

3. Establishment of plans for protecting

The heads of the relevant central administrative agencies in jurisdiction over critical information and communications infrastructures shall establish and implement a protection plan for critical information and communications infrastructures in their fields every year. The protection plan is prepared by synthesizing and coordinating the protection measures submitted by the management agency. Besides, the head of the relevant central administrative agency submits the next year's protection plan and new designation agenda for information and communications infrastructure to the Committee for Protection of Information and Communication Infrastructure for deliberation. The protection plan submitted to the committee is to be synthesized and adjusted through the deliberation process.

Figure 2-3-2-3 **Business procedure for protection of critical information and communications infrastructure**

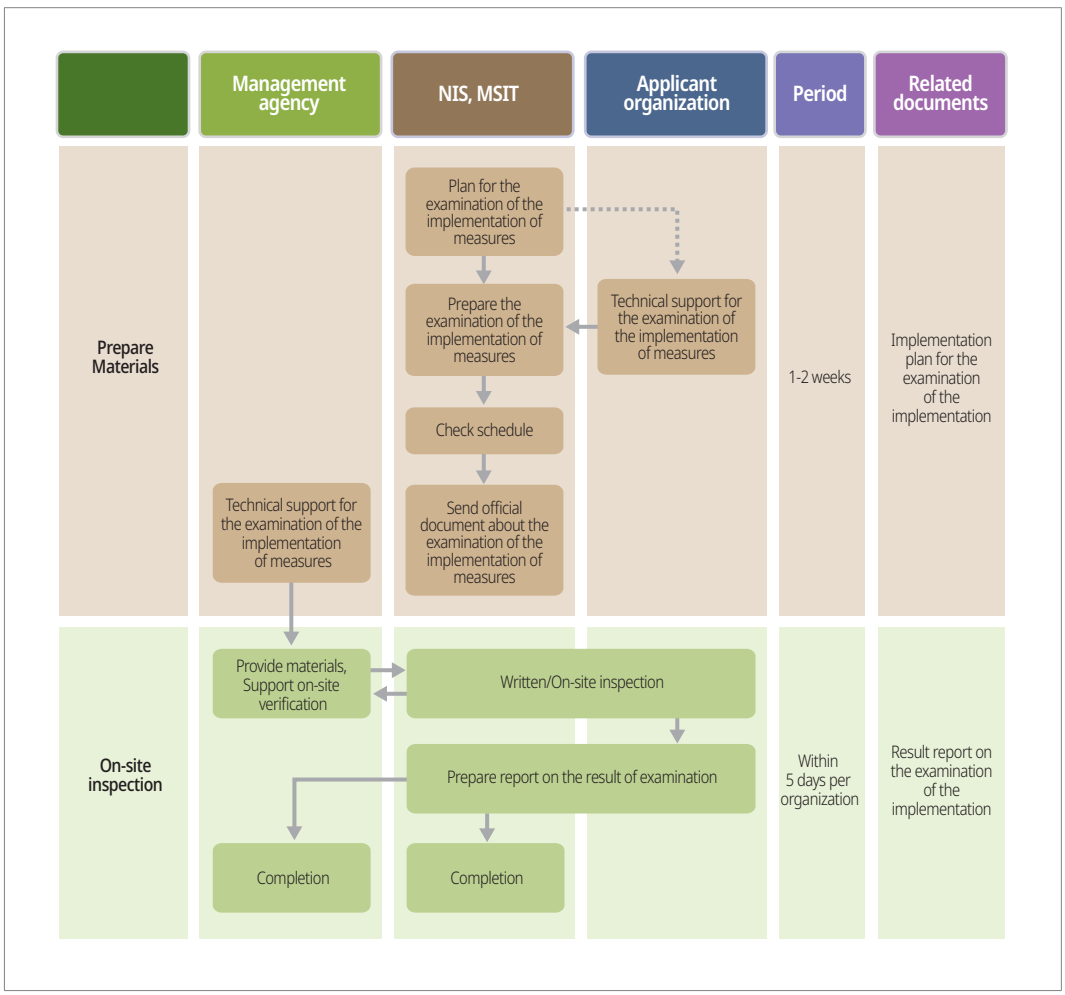


4. Ascertaining implementation of measures to protecting

The heads of state agencies prescribed by the Presidential Decree, such as the Director of the NIS and the MSIT, may confirm the implementation of measures to protect critical information and communications infrastructure with respect to the management agency. In addition, they may submit data necessary for confirmation of implementation and confirm and check the details of the protective measures. The examination of the implementation of the protection measures consists of a written inspection and an on-site inspection. To confirm whether the protection measures are implemented, the inspection is conducted based on the evaluation materials on the implementation of the protection measures submitted by the management agency and the checklist of the implementation of the measures. Moreover, the Director of the NIS

and MSIT shall report the results of confirmation of the implementation of measures to protect critical information and communications infrastructure to the Committee for Protection of Information and Communication Infrastructure. They may also recommend improvement to management agencies that they deem to be in need of supplementation.

Figure 2-3-2-4 **Procedures for confirming the implementation of measures to protect critical information and communications infrastructure**



5. Raising of public awareness of CIIP

A. Workshop for Infrastructure protection

Since 2004, the NIS and MSIT have held an annual Workshop for Critical Infrastructure Protection (WIPRO) to raise awareness of information protection and to strengthen the competence of critical information and communications infrastructure personnel.

In 2021, the workshop was conducted live online due to a social distancing campaign, and 326 infrastructure managers from 142 organizations attended to strengthen communications among infrastructure managers through an explanation of infrastructure protection policy, special lectures on information security technology, awards for merit, and sharing of public/private best practices.

Figure 2-3-2-5 Critical information and communications infrastructure protection workshop

Opening address by the MSIT

Awards for merit

B. Critical Infrastructure Security Forum

Since 2012, the Infrastructure Protection Forum has been operated to strengthen cooperation and expand information exchange among critical information and communications infrastructure management organizations.

In 2021, because of the COVID-19, about 270 key information and communications infrastructure information security officers from 92 management organizations participated in the forum online to explain infrastructure protection policy, share examples of excellent cyberattack response training organizations, and discuss major issues related to infrastructure and development plans for protection work.

Figure 2-3-2-6 Critical Infrastructure Security Forum

View of the conference hall

Sharing excellent examples

C. Cyber Attack Response Training

In September 2021, cyberattack response training against ransomware was conducted for 129 control systems of 57 management organizations for infrastructure. Training plans and scenarios were prepared and implemented with the aim of strengthening the control system management agency's effective cyberattack readiness and preparing an accident response and recovery system.

D. Infrastructure Cyber Security Contest

In 2021, the 3rd Cyber Security Contest for infrastructure management agencies was held online, hosted by the NIS and supervised by the NSR. 79 people from 40 teams in charge of infrastructure facilities in two fields of information and control systems participated in the contest. In the information system field, the 'Dogong' team of the Road Traffic Authority won the championship, and the 2nd place 'IIAC-orona' (Incheon International Airport Corporation) and the 3rd place 'Healthro 32' (National Health Insurance Corporation) won prizes. In the field of control system , Korea Electric Power Corporation's 'PowerScada' team won the championship, and 'Power Security' (Korea Electric Power Corporation) in the 2nd place and KOEN_IT (Korea South-East Power) in the 3rd place awarded prizes.

Figure 2-3-2-7 Infrastructure Cyber Security Contest

Grand Prize in information system field
(Road Traffic Authority)

Grand Prize in the control system field
(Korea Electric Power Corporation)

Section 3 Incident Cases

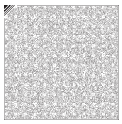
In the past, information and communications infrastructure was operated as a closed network, and most cases involved damage by physical attacks or manipulation errors. However, with the introduction of information and communications services to the information and communications infrastructure, damage from cyberattacks such as hacking, malicious e-mail, and distribution of ransomware are occurring frequently. Security incidents occur in various fields such as electricity, water resources, transportation, and finance, and may cause large-scale damage, including human and economic loss.

Table 2-3-3-1 Cases of domestic and international information and communications infrastructure infringement incidents

Time	Country of origin	Incident content	Remark
January, 2003	U.S.	• Slammerworm infiltrated a private computer network at the Davie-Besse nuclear power plant in Ohio, causing the safety monitoring system to shut down for 5 hours	Nuclear power
March, 2007	U.S.	• Destruction of generator by changing generator operation cycle in the power plant control system simulation hack supervised by the Department of Homeland Security (DHS)	Electric energy
August, 2007	U.S.	• A former employee installed a malicious program on the TCCA canal control system in California, paralyzing canal operation and resulting in a loss of more than $50 million	Water resources

Time	Country of origin	Incident content	Remark
January, 2008	Poland	• A 14-year-old boy modified a TV remote control to illegally manipulate a tram intersection, derailing 4 trams and injuring 12	Transportation
May, 2008	U.S.	• Successful penetration of the Internet power plant control system in a simulated hacking of the control system of TVA, the largest national power company in the United States, hosted by the Government Accountability Office (GAO)	Electric energy
August, 2008	Turkey	• Alarm management network failure due to network penetration using vulnerability of oil pipeline camera communications software, and inducing explosion accident by oil pressure modulation	Energy
August, 2009	Russia	• 75 died in an explosion of a generator turbine due to the failure of the turbine control system in a hydroelectric dam	Water resources
July, 2010	Iran	• Stuxnet virus invaded the control system of a nuclear power plant, causing a partial malfunction of the Natans nuclear centrifuge	Nuclear power
November, 2011	U.S.	• Illinois water system infiltration destroyed a pump operating system	Water resources
May, 2012	Iran, Sudan, Syria, etc.	• Intrusion into computers in major Middle Eastern countries to leak or destroy important data	Major facilities in the country
October, 2012	U.S.	• Power facility turbine control system infected with malicious code and stopped operating for 3 weeks	Electric energy
March, 2013	S. Korea	• A number of companies such as broadcasting and finance were damaged by computer network failures including system destruction caused by malicious code, causing damage to over 48,000 PCs and systems	Broadcast Finance
January, 2014	Japan	• A manager's PC in the Monju Nuclear Power plant in Fukui Prefecture was infected with a virus, and internal data such as education and training reports and organizational change publicity e-mails were leaked	Nuclear power
December, 2014	Germany	• Failure in the furnace control system of a steel company	Steel
December, 2015	Ukraine	• Control system service interrupted due to penetration of malicious code into a power plant, resulting in a power outage in 80,000 households	Electric energy
October, 2016	U.S.	• Hosting company Dyn's DNS service had website access failure due to DDoS attack	Communication
June, 2017	Japan	• WannaCry ransomware distributed to Honda Motors' Sayama plant; production halted for 48 hours	Manufacture
January, 2018	Japan	• Virtual assets service provider Coincheck hacked, causing 58 billion yen damage	Finance
May, 2018	Mexico	• Five banks hacked and $15.4 million withdrawn to fake accounts	Finance

Time	Country of origin	Incident content	Remark
November, 2018	U.S.	• At HSBC Bank's US branch, an unknown hacker gained illegal access to a customer's online account and leaked some information	Finance
January, 2019	U.S.	• Oklahoma Security Department leaked FBI investigation data through rsync service	Administration
March, 2019	U.S.	• S-Power, a solar and wind energy supplier, was attacked by a denial of service (DoS) attack due to a vulnerability in the Cisco firewall, and the connection with power generation facilities and 12 companies was interrupted	Energy
May, 2019	U.S.	• Baltimore attacked by ransomware, causing damage to files being encrypted	Administration
July, 2019	Republic of South Africa	• A ransomware attack occurred against City Power, a power supply company in Johannesburg, resulting in power outages in most regions and paralyzing the administration of electricity bills	Electric energy
September, 2020	Germany	• An unknown hacker infected the network of Düsseldorf University Hospital with ransomware, causing service interruption and death of one severely ill patient while evacuating to another hospital	Hospital
December, 2020	U.K.	• People's Energy, a power supply company in Scotland, was hacked and leaked personal information of 270,000 people	Electric energy



Chapter 4

National Cybersecurity Coordination

Section 1 Incident Response

1. National Security Operations Center

The Ministry of Science and ICT (MSIT) and the Korea Internet & Security Agency (KISA) operate the Korea Computer Emergency Response Team Coordination Center (KrCERT/ CC) to prevent and respond to Internet security incidents for private sector, and monitor abnormal events in the domestic network, respond to security incidents, and, if necessary, work together with local and global organizations.

The security operations center of the KrCERT/CC constantly monitors the traffic status of the domestic network, major DNS (Domain Name System) services, and the web server connection status of major domestic institutions in the private, public, and financial sectors. It receives reports on DDoS (Distributed Denial of Service) attacks, phishing, smishing, and homepage defacements. Moreover, it accesses risks against novel malware and security vulnerabilities in domestic networks.

To effectively respond to cyberattacks against mission-critical services like the COVID-19 vaccination, Tokyo Olympics, and Korea Sale Festa, The KrCERT/CC

incorporated the emergency response system with vigilant security monitoring, cooperation hotlines, and security incident analysis support. In particular, as the ransomware, which encrypts data by hacking and demands money in exchange for unlocking, increases, the KrCERT/CC enhanced the ransomware response capability by establishing a report site for ransomware-only and 'Ransomware Response Support Team'. In addition, the KrCERT/CC maintained incident response cooperation relationships with information and communications services providers (ISP, IDC, telcos, MSO, etc.), security companies, and related organizations for information sharing and emergency response.

2. Detect and respond to web-based malware

As HTTP-based malware distribution has increased since 2006, the government has maintained a detection and response system against web-based malware. Furthermore, it has strengthened the detection and response of malicious codes by inspecting forgery and falsification of dedicated programs on web hard sites and free domestic software (about 200).

The web-based malware detection system inspected 77,000 domains in 2006 and continued to expand to 4.1 million in 2021.

Table 2-4-1-1 **Inspection targets of web-based malware**

(Unit of measurement: ten thousand units)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Inspection targets	7.7	10	12	20	100	180	200	230	250	280	340	370	340	380	400	410

※ 4.1 million domestic domains: 3.2 million ccTLD (.kr, Korea) and 0.9 million gTLD (.com, .net, .name, etc.)

Detections of web-based malware increased by 17% (6,034 → 7,043) compared to 2020.

Table 2-4-1-2 **Detection and response of web-based malware**

(Unit of measurement: ten thousand units)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Distribution site	993	1,619	1,324	1,731	1,434	1,433	3,270	4,472	2,583	3,295	1,370	1,197	856	566	738	2,584
Staging site	5,624	3,932	7,654	5,621	5,240	10,372	9,748	13,278	45,120	43,555	9,674	12,150	13,898	7,733	5,296	4,459
Total	6,617	5,551	8,978	7,352	6,674	11,805	13,018	17,750	17,703	46,850	11,044	13,347	14,754	8,299	6,034	7,043

※ Distribution site : Malicious code distribution website
※ Staging site : Homepage leading Internet users to a distribution website

Among the types of web-based malware distributed through the homepage, credential stealers targeting account information and device information (41.8%) were the highest. In addition, dropper and downloaders (12.2%), ransomware/crypto-miner (5.3%), RAT (4.2%), and DDoS attacker (4.2%) were found in order.

In the case of overseas distribution sites, cooperation with major domestic Internet service providers (ISPs) was blocked to prevent domestic users from being exploited. Moreover, in the case of the domestic staging site, the website operator was notified by phone, e-mail, or official letters along with the technical recommendations to remove the malicious code.

3. Response to DDoS attacks

A Distributed-Denial-of-Service (DDoS) attack overloads machine or network resources unavailable by disrupting the services of a host connected to the Internet. The DDoS attacker makes use of a herd of infected computers controlled via command and control servers. Therefore, it is necessary to filter malicious traffics and to remediate the infected machine.

The KISA provides the DDoS Shelter Service, which mitigates DDoS attack traffics to the website of small and medium-sized companies.

The need for the DDoS Shelter arose after 3.4 DDoS attacks in 2009 and the deployment of the DDoS Shelter completed in 2010. Since its initial deployment, it has provided 22,800 services mitigating 1,350 DDoS attacks by 2021.

Table 2-4-1-3 **DDoS Shelter Service**

(Unit of measurement: cases)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
Service users	52	101	175	260	413	593	1,012	1,640	2,854	3,839	4,590	7,271	22,800
DDoS attack defense	25	60	138	116	110	83	96	87	126	167	235	107	1,350

Furthermore, the KISA presents a malware removal service for critical nationwide malware infections. It directly notifies the infection to the users of the infected machine and provides customized antivirus software. More specifically, it informs the

infection to the user via the browser pop-up windows where the antivirus software installation instruction is located. At the same time, it induces treatment by providing a customized, exclusive vaccine, which can treat the malicious code that infects the PC.

In 2021, it handled 212 cases notifying 135,747 infected machines and distributed 144 exclusive malware remover.

Table 2-4-1-4 Infected PC Cyber Treatment Systems

(Unit of measurement: cases)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
Infection notifications	9,404,759	61,347	64,206	248,281	110,413	47,776	124,310	106,525	267,456	381,492	135,747	10,952,312
Exclusive malware remover	54	51	57	67	74	82	92	103	113	127	144	964

4. Response to cyberattacks in financial sectors (phishing, pharming, smishing)

A. Phishing response

In cybersecurity, phishing is social engineering attack sending fraudulent messages to trick human victims into revealing sensitive information such as personal information (ID/PW) and financial information (security card, public certificate information). It lures a user through email or text messages to a rogue website designed as a regular financial and public institution, enticing users to reveal credentials for financial transactions.

The KISA operates a cyber fraud response system to detect the rogue website used for phishing scams.

The KISA works with VeriSign, a domain registrar of .com and .net, to operate a phishing site detection system against new domain names registered and deal with phishing scams, which often use .com and .net TLD to bypass Korean jurisdictional control. In 2014, it upgraded the system so that it can also verify newly registered .kr domains.

B. Smishing response

Smishing is phishing over text messaging and appears since 2012. Attackers lure victims to install malicious apps through a fraudulent message with a link (URL) of an ostensibly trusted person, company, or public institution. With the fast growth of smartphone users and potential victims, the smishing technique evolves rapidly. In response to the growing smishing attacks, the KISA operates a smishing response system since 2014.

The KISA provides both technical and policy-based responses to minimize the loss from the smishing attacks. It deploys a smishing response system and the cyber trap as technical measures. The smishing response system collects suspicious text messages from multiple sources then activates the URL to verify the downloads of malicious apps. To overcome the limitations of the passive system, it exposes false personal information to the virtual honeypot to collect suspicious criminal activities before it affects the public. Information gathered from the systems is used to filter the IP addresses of staging and exfiltration servers to contain the damage.

Moreover, the KISA is working together with companies 'WhoWho' and 'Alyac M2.0' to provide service for users to verify the authenticity of the text messages sent from seemingly suspicious sources. In 2020, the KISA planned to share the Indicator of Compromise (IoC) of identified smishing information to ISP and other companies in the private sector.

5. Response to mobile malware

Mobile malware (malicious apps) began to spread on a large scale from the second half of 2012 and increased rapidly from 2013. In 2014, a beta version of the 'mobile threat quick response service' was developed to notify and remediate the mobile phone infected by malicious apps, and a year later, KISA launched the service with the cooperation of 3 major mobile carriers (KT, SKT, and LGU+) in Korea.

Mobile threat quick response service provided service to the subscribers with the cooperation of the communication service provider with the user subscription. The system analyzes the C2, staging, and exfiltration site of the malicious app to extract IoC information. Based on the analysis results, the system notifies the infection of the victimized mobile users to remove the malicious apps through the services. The

users receive the notification through the pre-installed security apps or the text message from the agency. In 2021, the system identified and informed 43,797 infected smartphones.

Table 2-4-1-5 Mobile Threat Quick Response Service

(Unit of measurement: cases)

	2015	2016	2017	2018	2019	2020	2021	Total
Number of notifications (based on devices)	24,517	27,608	47,152	20,277	29,752	54,533	43,797	247,636

Section 2 Incident Prevention

1. Domestic activities

The KISA is working closely with major telecommunication companies, e.g., ISP, IDC, mobile service providers, MSO, cybersecurity companies, and other institutions to manage the national cybersecurity risk in private sectors. It includes incident response cooperation, field-centric practical policy-making based on communication, and building cooperative cyberattack defense architecture through facilitating cyber threat data exchange.

A. Cyber threat intelligence network

Cybersecurity is a field that needs private and public cooperation more than any other field to solve the problem. To cope with the problem together, the KISA has operated a 'cyber threat intelligence network' with Korean cybersecurity companies (AhnLab, Est security, Hauri, INCA Internet, NSHC, Bitscan) since December 2014. In 2021, this network group held a cooperative meeting with overseas CERTs such as Thailand and Japan to discuss increasing global issues. Moreover, this network group analyzed and predicted the trend of cyberattacks in 2022 and jointly announced the 'Cyber Threat Analysis 2021 and Outlook 2022'.

B. Cyber threat information analysis and sharing system

The Cyber Threat Analysis & Sharing (C-TAS) is a Cyber threat intelligence sharing system run by the KISA since August 2014. As of December 2021, 332 organizations, including cybersecurity-related organizations, companies, and portal companies, are participating and sharing 329 million cyber threat information items.

It analyzes collected malware and vulnerability data to generate IoCs for security products. Malicious URL and IP data are shared with the participant organizations to filter the harmful contents.

C-TAS had operated a two-way information sharing policy as a membership condition. However, it decided to switch to an open type so that more companies can refer to cyber threat responses. Accordingly, it built an open C-TAS homepage to provide various types of customized information according to positions and job characteristics, such as security practitioners and managers, so that many companies, including SMEs, can utilize cyber threat information. Furthermore, it plans to provide an emergency dissemination system to minimize damage to businesses by quickly disseminating emergency response-related information through text messages (SMS) or alerts (SNS).

C. Cybersecurity Big Data Center

The KISA opened the Cybersecurity Big Data Center in December 2018. It uses AI and big data to predict, detect and respond to fast-evolving security threats.

The center collects cyber threat data from various domestic and global sources, e.g., domestic and international public sector, commercial intelligence, open-source intelligence, and the C-TAS.

In 2021, the Cybersecurity Big Data Center established two types of data sets in the cybersecurity field (malware code and intrusion incident), which are in high demand in the private sector, and laid the foundation for the use of AI data in the private sector. It not only collects threat information, but also performs various tasks for all cycles (collection → processing → labeling) of AI data set construction, opening the data set on a trial basis to desired companies such as the public, telecommunication, and gaming other than the security field. In this way, the center supports the strengthening

of cybersecurity based on public-private collaboration.

Moreover, the center provides a 'platform for cybersecurity big data utilization', an improved version of the existing platform, for anyone interested in cybersecurity. As such, private companies, schools, and research institutions can make use of big data for their own purposes. The center is striving to promote the use of cybersecurity AI and big data by providing an analysis environment not only offline but also online.

The Cyber Security Big Data Center carries out various activities to strengthen the ability to use AI and big data based on the participation of the public, such as contests. The center is continuously promoting the expansion of the base for the use of big data in the cybersecurity field by analyzing and utilizing AI and big data using collective intelligence, discovering new models, and sharing results through the contest for cybersecurity AI and big data.

D. Designate and register chief information security officer

According to Article 45-3 of the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.,」 (hereinafter, the 'Information Communications Network Act'), information and communications service providers must designate a Chief Information Security Officer (CISO) at the executive level and report it. As of the end of 2021, there are 24,000 companies with designated and reported CISOs.

Regarding this, the KISA supports prevention, response, and cooperation activities through the CISOs. In 2021, the KISA sent a total of 29 e-mails to share information on security issues and disseminate preventive measures to the CISOs in order to strengthen the ability to respond to cyber threats. In addition, the KISA conducted the common courses, as well as, distribution and manufacturing training courses online at all times to strengthen the capabilities of the CISO, and approximately 12,000 people participated in the courses.

Moreover, the Korea Council of Chief Information Security Officers, organized in accordance with Article 45-3, Paragraph 5 of the 「Information Communications Network Act」, held the CISO Forum and the CISO Workshop to exchange information between CISOs.

In 2021, the National Assembly passed an amendment that diversifies the uniform status of the CISO, rationalizes the scope of reporting, and eases restrictions on working in dual roles. Besides, the National Assembly entrusted specific matters regarding the scope and status of the report of the CISO to the Presidential Decree, and it came into force along with the revision of the Enforcement Decree in December 2021.

Accordingly, the mandatory designation of a uniform 'executive level' to companies with the duty to report the CISO was changed to a 'director' for large-scale corporations subject to the restriction on concurrent positions. Furthermore, it became possible to designate a person in charge of information protection (head of a department) for general reporting obligations of 'medium-sized companies' that need information protection. Previously, all medium-sized enterprises and above were subject to the reporting obligations. However, among medium-sized enterprises, only telecommunication service providers, personal information controllers, mail order distributors, and information protection management system certification operators became subject to the mandatory reporting requirements.

Meanwhile, for companies exempted from reporting obligations, such as those with a capital of 100 million won or less and small businesses, the owner or representative is regarded as the CISO to prevent any gap in cybersecurity.

E. Regional Information Security Center

The KISA has 10 Regional Information Security Centers in operation for each region throughout the country in connection with the local governments since 2014 to improve regional cybersecurity posture. The Centers are located in Incheon, Daegu, Honam, Jungbu, Dongnam, Gyeonggi, Ulsan, Gangwon, Gyeongbuk, and Chungnam.

The Regional Information Security Centers provide cybersecurity consultation services and support installation cost of cybersecurity products for local SMEs who have difficulties securing cybersecurity budgets, and support cloud-based cybersecurity services for small businesses with small-scale ICT assets who cannot afford consultation services.

Also, the Centers provide cybersecurity education programs for free to local SMEs and university students who study cybersecurity, which the classes are customized by the skill levels of the attendance, beginner and intermediate courses.

2. Cybersecurity International Cooperation

A. Bilateral and multilateral cooperation with global organizations

The Korea Internet Security Center in the KISA acts as a CERT with national responsibility. In 2011 KrCERT/CC in Korea, CNCERT/CC in China, and JPCERT/CC in Japan signed an MoU for tighter cooperation. The MoU dictates annual meetings, sharing best practices and experiences of incident responses and discussing areas for improvement in each country. Recently under the circumstances of COVID-19, they share related cyber threats and responses in the northeast Asian region.

Section 3 ISMS, PIMS, ISMS-P

1. Overview

In the 4th Industrial Revolution era, emerging technologies, e.g., blockchain, cloud, 5G, and IoT are changing every aspect of our lives. As new technologies become closer to real life and their importance increases, extensive personal information breaches from the credit card company, a security breach in virtual currency exchange, and service disruption in a cloud computing environment due to cyberattacks are arising. The recent trend in cyberattacks is moving from non-discriminative to targeted attacks. Adversaries aim at specific corporate or personal information with highly advanced skills and tactics, causing significant social and economic aspects. It includes sensitive data breaches in high-tech companies, corporate credibility churn, negative effects on stock prices, and collective lawsuits for damage compensation for the security breach. The technic-centric, temporary patchwork approaches show their limitation for today's evolving cyber threats, and it is necessary to have fundamental changes to have them under control.

Personal information & Information Security Management System (ISMS-P) certification presents a standard model and certification criteria for the management system established by companies or organizations to prevent cyberattacks and

personal information leakage. In terms of acquiring the certification, a company or institution wishing to be certified is evaluated through an independent and objective third-party certification/assessment agency to determine whether the company or institution is suitable for continuous operation of ISMS-P and whether it complies with ISMS-P certification standards. For fairness and objectivity of the certification system, the KISA plays the role of a legal certification body. The Financial Security Institution also plays the role of a legal body designated by the MSIT. Moreover, the Korea Association for ICT Promotion, the Telecommunications Technology Association, and the Online Privacy Association were designated as screening agencies. As the number of certificate targets and fields increases, the government plans to expand the authentication agencies and audit agencies gradually. From 2021, the procedure for designating audit agencies is always in operation through the application of the desired agency.

The ISMS certification system started in 2001, and the first certificate was issued in 2002. In 2013, the government made it mandatory for major communications service providers to be subjects for the ISMS certification. It has been continuously expanded to non-profit organizations like universities with over 10,000 enrolled students, and large hospitals whose revenue was over 150 billion KRW.

The government consolidated the Personal Information Management System (PIMS) and the ISMS in 2018 as the cyber threats kept evolving to advanced and converged. It promulgates the ISMS-P certification standard as an integrated certification system.

The government amended the notification in order to effectively respond to the increasing number of companies or organizations seeking ISMS-P certification and the emergence of new technologies such as virtual assets and cloud infrastructure. Accordingly, an audit agency was designated at all times, and the quality of authentication and audit could be improved through the follow-up management of the designated authentication and audit bodies. Also, it became possible to respond to the event of an urgent disaster or disaster.

Figure 2-4-3-1 Overview of ISMS-P certification

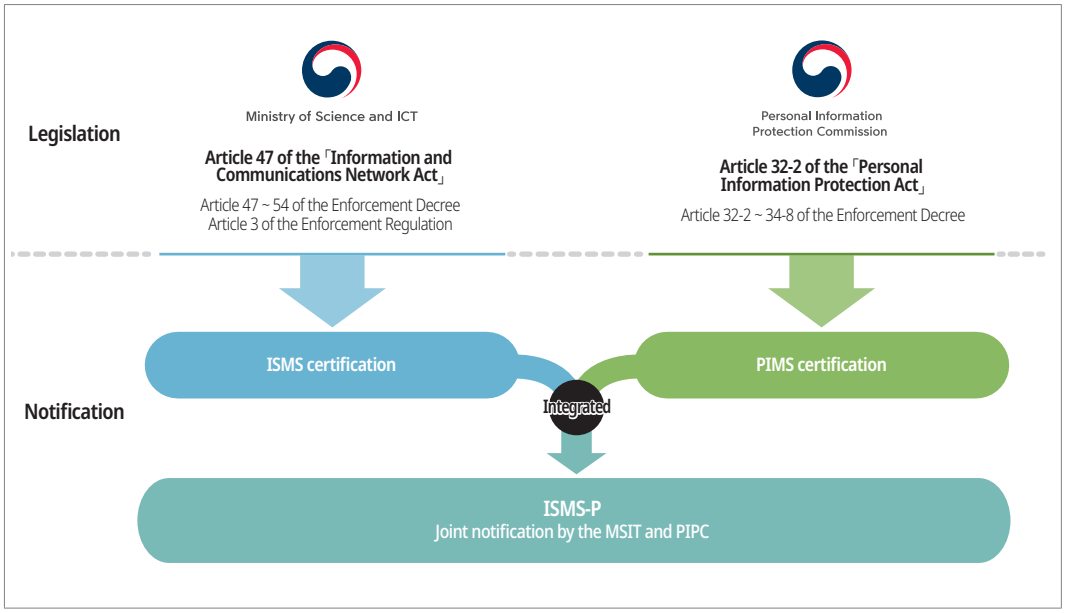


Table 2-4-3-1 ISMS-P certification system progress

Year	Content
2001	• Executive Summary of ISMS certification system (Article 47 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」)
2002	• Notification of certification screening standards (Notification No. 2002-22 of the Ministry of Information and Communication) • First certificate issuance
2004	• Executive Summary of a safety diagnosis system for cybersecurity (Article 46-3 of the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」)
2011	• Revision of ISMS certification standards (existing: 137 control items → revision: 104 control items) • Introduction of PIMS (Personal Information Protection Management System) certification system
2013	• Unification of information security safety diagnosis system into ISMS certification system • Designation of major information and communications service providers, etc. as obligatory targets • Unified ISMS certification system and G-ISMS certification system • Enforcement of personal information security management system (Article 47-3 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」)
2014	• Designated as ISMS audit organization ※ Korea Association for ICT Promotion (2014. 5.), Telecommunications Technology Association (2015. 2.)
2015	• Additional designation of ISMS certification body ※ Financial Security Institute (2015. 7.)

Year	Content
2016	• Expanding ISMS certification obligation to medical and education fields ※ Article 47 of the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 49 of the Enforcement Decree
2018	• Integration of ISMS and PIMS certification system ※ 「Notification on information security and personal information security management systemcertification, etc.」 (Ministry of Science and ICT Notification No. 2018-80) amendment (2018. 11.)
2019	• Designation of ISMS-P certification body and audit body ※ Certification body (Financial Security Institute), audit body (Telecommunications Technology Association, Korea Association for ICT Promotion) (2019. 7.)
2020	• Designation of ISMS-P audit body ※ Online Privacy Association (2020. 2.)
2021	• System improvement such as permanent designation of ISMS-P examination agency, follow-up management, and establishment of exceptions in case of disaster ※ 「Notification on information security and personal information security management system certification, etc.」 (Ministry of Science and ICT Notification No. 2021-27)amendment (2021. 3.)

Table 2-4-3-2 ISMS-P certificate maintenance

	2013	2014	2015	2016	2017	2018	2019	2020	2021
(old) PIMS	28	27	41	63	71	76	35	22	137
(old) ISMS	272	377	415	470	517	601	584	349	10
ISMS-P	-	-	-	-	-	-	136	464	789
Total	300	404	456	533	588	677	755	835	936

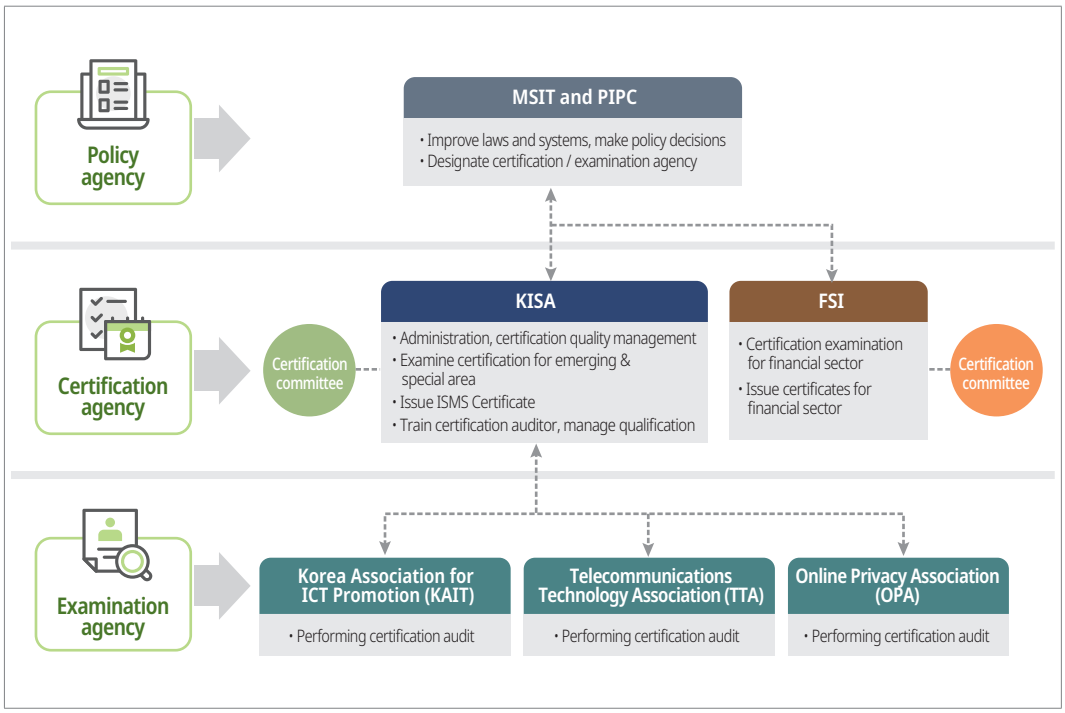
2. Promotion system

The ISMS-P certification promotion system consists of a policy agency (council), certification and examination agency, certification committee, and certification reviewer. The MSIT and the Personal Information Protection Commission (PIPC) are responsible for improving laws and systems, making policy decisions, and designating and supervising certification/examination agencies as policy bodies. And, as a legal certification body, the KISA plays a role in certification examination, operation of the certification committee, issue and management of certificates, and improvement of certification systems and standards.

The certification committee deliberates on the certification examination results and the validity of the cancellation of certification. It comprises no more than 35 members with knowledge and experience in cybersecurity, such as cybersecurity experts and

information system supervisors. The certification agency selects certification auditors from experts in each field who have acquired the auditor qualification.

Figure 2-4-3-2 ISMS-P Certification Promotion System



3. Certification subject and procedure

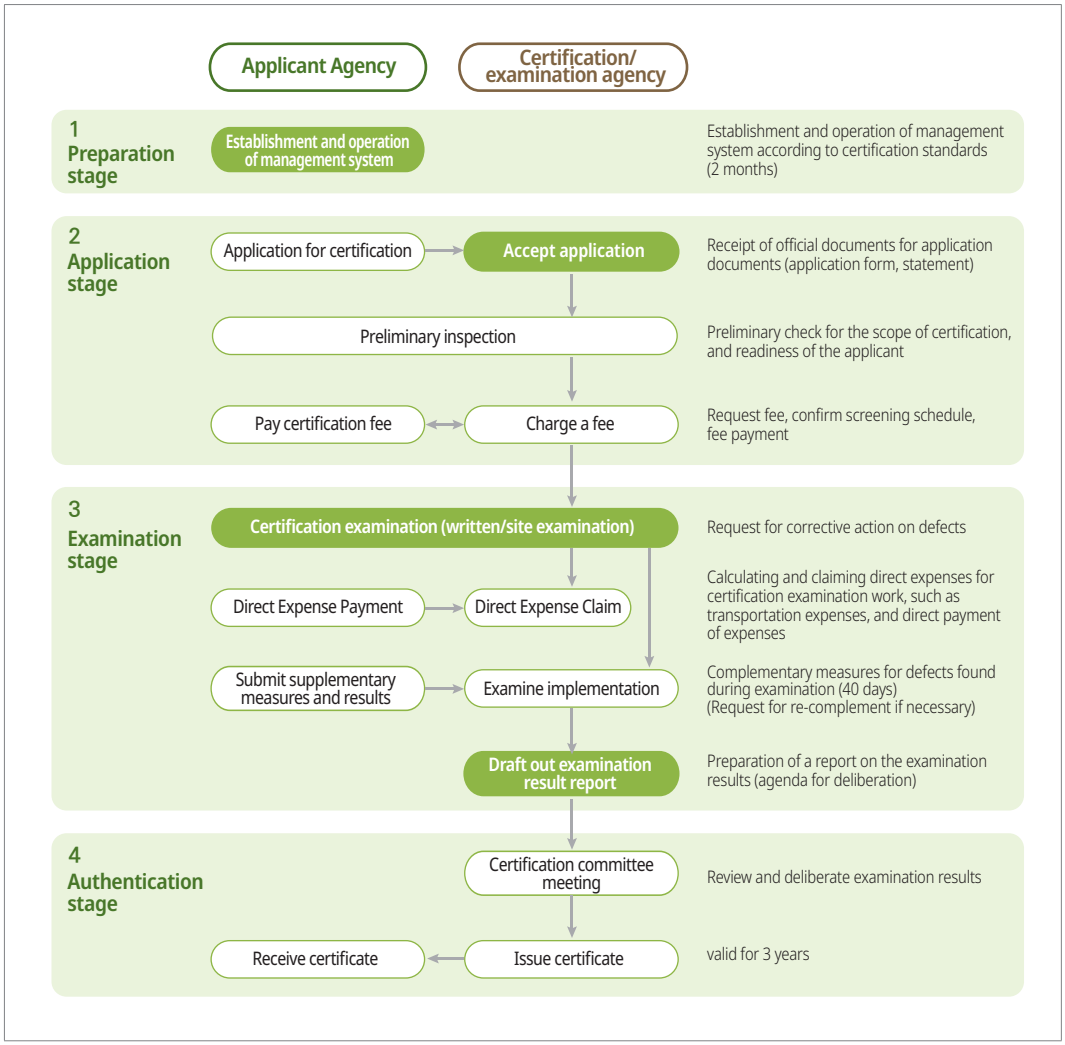
According to Article 47 (2) of the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」, the obligated organization must obtain ISMS or ISMS-P certification. A fine is imposed when there is a violation of the regulation.

Table 2-4-3-3 Standards for ISMS obligated persons

	Mandatory
ISP	• Enrolled communications service provider in Seoul and all metropolitan city in accordance with Article 6, Paragraph 1 of the 'Telecommunications Business Act'
IDC	• The business entities of clustered information and communications facilities in accordance with Article 46 of the 'Act on promotion of information and communications network utilization and information protection, etc.'
Companies/ persons who meet the requirement for sales or number of users	• Companies or persons with more than 100 billion KRW in turnover of information and communication service part.
	• Companies or persons with more than 1 million users of information and communication service per day in the last 3 months of the previous year
	• Companies or persons with more than 1500 billion KRW in turnover/tax revenue (where applicable) - Tertiary hospitals in accordance with Article 3-4, of the 'Medical Service Act' - Schools with more than 10000 students on December 31 of the previous year in accordance with Article 2, of the 'Higher Education Act'

ISMS-P certification is for those who need both flow of personal information and a cybersecurity certificate. On the other hand, ISMS is for those who need only the cybersecurity certificate. Once the subjects select the type of certificate, they need to consult with the KISA or other authorities for the scope of the process. The auditor from the certificate authority should visit the organization for written and on-site examinations. The auditee organization should rectify the identified deficiencies for issuing the certificate.

Figure 2-4-3-3 ISMS-P authentication procedure



4. Certification criteria

ISMS certification consists of management framework setup & compliance (16 items) and protection plan requirements (64 items). The ISMS-P certification criteria are composed of the ISMS certification criteria (80 items) and requirements for each stage of personal information processing (22 items).

Table 2-4-3-4 **ISMS-P criteria**

Certification		Category	Criteria
ISMS-P (102)	SIMS (80)	1. Management framework setup & compliance (16)	1.1 Management framework infrastructure setup (6) 1.2 Risk management (4) 1.3 Management framework compliance (3) 1.4 Management framework - checkup and improvement
		2. Protection plan requirements (64)	2.1 Policy, organization, assets (3) 2.2 Human resource security (6) 2.3 External staff security (4) 2.4 Physical security (7) 2.5 Authentication & Authorization (6) 2.6 Access Control (7) 2.7 Encryption (2) 2.8 System deployment & development security (6) 2.9 Systems and services management (7) 2.10 Systems and services security (9) 2.11 Incident prevention & response (5) 2.12 Disaster recovery (2)
	-	3. Requirements for each stage of personal information processing (22)	3.1 Security measure on personal information gathering (7) 3.2 Security measure on retaining/using personal information (5) 3.3 Security measure on personal information provision (3) 3.4 Security measure on personal information destruction (4) 3.5 Personal information subjects' right protection (3)

Section 4 Cloud Security Assurance

1. Overview

By the Cloud Security Assurance Program by Article 23 (2) of the 「Act On The Development Of Cloud Computing And Protection Of Its Users 」, when cloud service providers request if their service complies with the cybersecurity standards, the certificate authorities assess and certify that they meet the requirement and the users can use the cloud service with assurance.

The Cloud Security Assurance Program certifies either one of the cloud services among information system infrastructure, application program, and development environment using cloud computing technology.

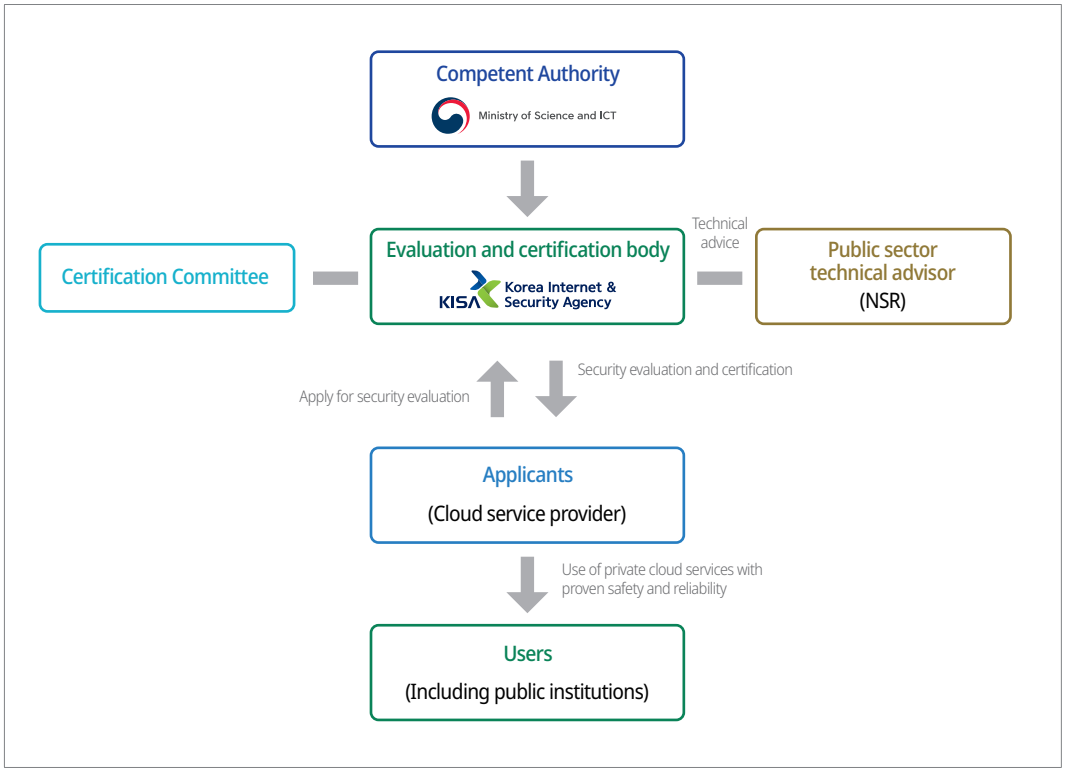
By the objective and fair Cloud Security Assurance Program operated by public institutions, cloud services provided by private sector are verified as safe and reliable, and address customers' security concern and secure competitiveness.

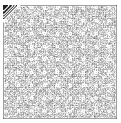
2. Security Evaluation and Certification

Security evaluation and certification on cloud services is divided by roles and responsibilities: competent authority, evaluation and certification body, certification committee, technical advisor, applicant, and user.

The competent authority is the Ministry of Science and ICT (MSIT), the evaluation and certification body is the Korea Internet & Security Agency (KISA), and the technical advisor is the National Security Research Institute (NSR).

Figure 2-4-4-1 Evaluation and certification on cloud security service





3. Certifications and Criteria

A. IaaS Security Certification

In order to operate cloud services, various infrastructures such as servers, storage, networks, and databases are required. Infrastructure as a Service (IaaS) provides these services for easy and convenient use in a virtual environment.

IaaS certification is evaluated based on a total of 117 control items including administrative, physical, and technical security measures and additional security measures for public institutions so that SaaS and DaaS operators can use them in such an environment.

B. SaaS Security Certification

Providing an application program running in a cloud environment in the form of a service is called SaaS (Software as a Service). By using this, it is possible to provide various services such as a website, video conferencing system, and e-approval system.

As SaaS can provide a variety of services, so that the certification is provided in two grades; simple grade and standard grade, based on inclusion of sensitive data. Regarding standard grade, if one or more of the five items, e-approval, accounting management, human resource management, security service, and PaaS (Platform as a Service) that deal with sensitive data are included, a standard grade must be issued. All other services can be certified as simple grade, and standard grade has 78 control items while simple grade has 30.

C. DaaS security authentication

Desktop-as-a-Service (DaaS) is a cloud service that provides a remote virtual PC environment. The advantage of DaaS is that one can access the personal work environment from multiple devices anytime, anywhere as it becomes possible to access the personal PC through the network.

Recently, as teleworking has been a trend due to the COVID-19, cases of using DaaS to access company networks are increasing. As the network used by the company can be accessed from the outside, there is a high possibility that data inside the company

will be leaked to the outside. In order to ensure security in such an environment, security certification is implemented based on 110 control items.

4. Evaluation Process

Security certification for cloud services can be divided into three stages: preparation stage, evaluation stage, and certification stage. After the evaluation body visits the applicant and conducts written/on-site evaluation, vulnerability check, etc., if nonconformities are identified, the applicant shall make up for all nonconformity items within 30 days (up to 90 days in case of extension). When all items are corrected, the certification committee has a deliberation session and decides whether to issue a certificate or not.

Figure 2-4-4-2 Evaluation process of security certification for cloud services

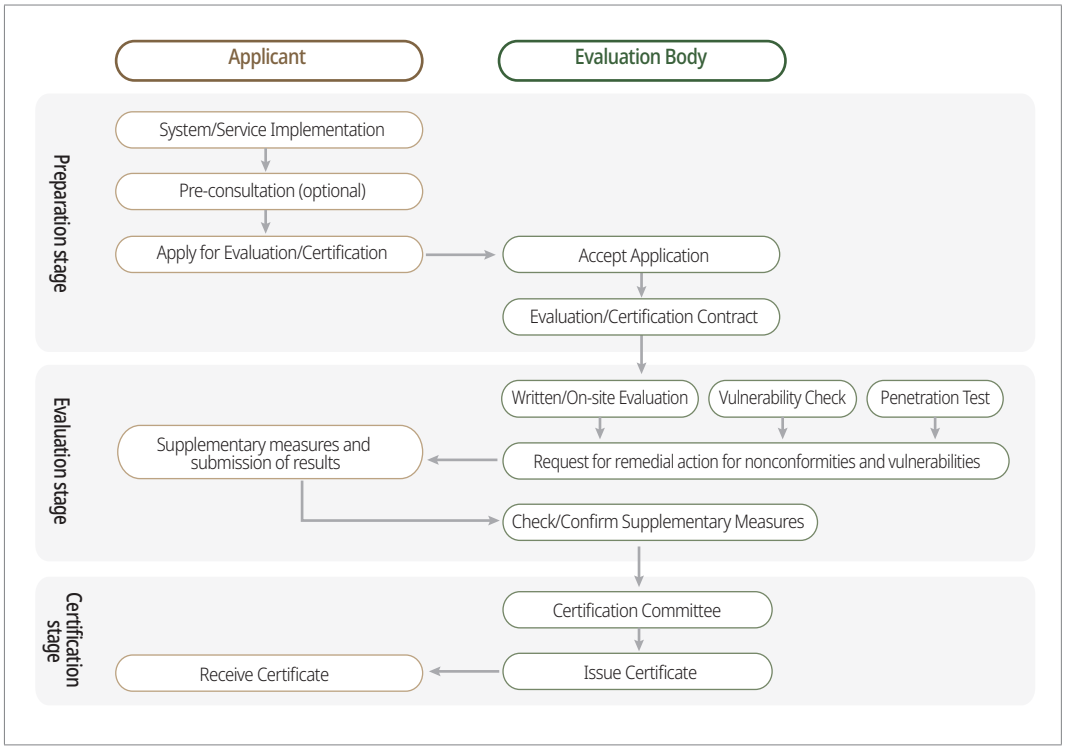


Table 2-4-4-1 Criteria for security authentication of cloud service

Field	Items	Number of items			
		IaaS	SaaS (standard)	SaaS (simple)	DaaS
1. Information security policy and organization	1.1 Information Security Policy	3	3	-	3
	1.2 Information Security Organization	2	2	2	2
2. Human Security	2.1 Internal personnel Security	6	4	1	4
	2.2 External Personnel Security	3	-	-	3
	2.3 Information Security Education	3	1	1	1
3. Asset Management	3.1 Asset Identification and Classification	3	1	-	3
	3.2 Asset Change Management	3	1	-	3
	3.3 Risk Management	4	1	-	4
4. Service Supply Chain Management	4.1 Supply Chain Management Policy	2	2	-	2
	4.2 Supply Chain Change Management	2	1	-	2
5. Intrusion Accident Management	5.1 Incident Procedure and System	3	3	1	3
	5.2 Response to Incidents	2	2	1	2
	5.3 Follow-up	2	2	-	2
6. Service Continuity Management	6.1 Disaster Response	4	4	1	4
	6.2 Service Availability	3	2	1	3
7. Conformity	7.1 Compliance with Laws and Policies	2	1	1	2
	7.2 Security Audit	2	2	-	2
8. Physical Security	8.1 Physical Protected Areas	6	-	-	6
	8.2 Protection of information processing facilities and equipment	6	-	-	6
9. Virtualization Security	9.1 Virtualization Infrastructure	6	2	1	5
	9.2 Virtual Environment	4	4	-	2
10. Access Control	10.1 Access Control Policy	2	2	1	2
	10.2 Access Rights Management	3	3	-	3
	10.3 User Identification and Authentication	5	5	4	5
11. Network Security		6	5	2	6
12. Data Protection and Encryption	12.1 Data Protection	6	6	2	6
	12.2 Media Security	2	-	-	2
	12.3 Encryption	2	2	2	2
13. System development and introduction security	13.1 System Analysis and Design	5	5	1	5
	13.2 Implementation and Testing	4	4	1	4
	13.3 Outsourced Development Security	1	1	-	1
	13.4 System Introduction Security	2	-	-	2
14. Additional Security Requirements for the Public Sector		8	7	7	8
Total		117	78	30	10

Section 5 Convergence Security

ICT convergence such as smart factories, smart cities, and autonomous vehicles that incorporate ICT to increase productivity and efficiency of existing industries is expected to further accelerate. With the acceleration of ICT convergence services, cybersecurity threats are transferred and expanded to threats from traditional industries, causing direct damage to people's lives and safety and the economy as a whole. Cyber incidents are already occurring worldwide in the field of smart factories and smart cities, and security vulnerabilities are being discovered in various convergence services such as autonomous vehicles. Accordingly, the government prepared the 'National Convergence Security Plan for '5G+ Core Service' (October 2019) to prevent security threats from the development and implementation stages of ICT convergence devices, products, and services. And, as part of that policy task, the government is building and operating the development of five major convergence services* security model and security living lab.

* five major convergence services are smart factory, autonomous vehicle, smart city, digital healthcare, and realistic content. These are 5G+ core services derived from the 5G+ strategy (April 2019) in consideration of marketability, competitiveness, and the need for policy support.

1. Convergence Service Security Model

The expansion of ICT convergence poses a risk that cybersecurity threats may be extended to core service areas and may cause direct damage to people's lives and safety and the economy as a whole. Accordingly, to strengthen security from the product and service development stage in the five major convergence service fields, the Ministry of Science and ICT (MSIT) has developed a security model that allows convergence service companies to develop and operate safe products and services. This security model diagnoses security threats with vulnerability checks and security tests and can be applied to each field. This security model also presents security measures such as security requirements, security technologies and solutions to respond to security threats derived from each convergence service field. This security model presents security measures such as security requirements, security technologies and solutions to respond to security threats derived by each convergence service field. The

first version of the security model was developed in December 2020 to test the security model in the convergence service industry site. In December 2021, the second version of the security model, which suggests security measures by extending the scope of protection for convergence services, was prepared and distributed to be used in industrial sites.

Figure 2-4-5-1 Convergence Service Security Model

2. Five Major Convergence Services for Security Living Labs

Security Living Lab is a space where convergence security consumers and companies can verify necessary security technologies and test the security of convergence service devices and platforms. The Lab was established in 5 special convergence industry areas in cooperation with the government in charge of convergence industry and the related organizations to allow more companies at the site can use it, and each area represents each of the 5 convergence industries.

The smart factory was built in conjunction with the demonstration factory of the Smart Manufacturing Innovation Center located in the Ansan city, Gyeonggi-do province. Based on the real hacking incident scenario of a smart factory, the factory provides users a set of security threats such as robotic process malfunction, and numerical errors in production. Users are also allowed to have security tests on smart factory solutions and equipment such as industrial wired/wireless facility, including PLC/HMI.

Security Living Lab for the autonomous vehicle was established in conjunction with the Saemangeum autonomous driving test bed located at the Jeonbuk Institute

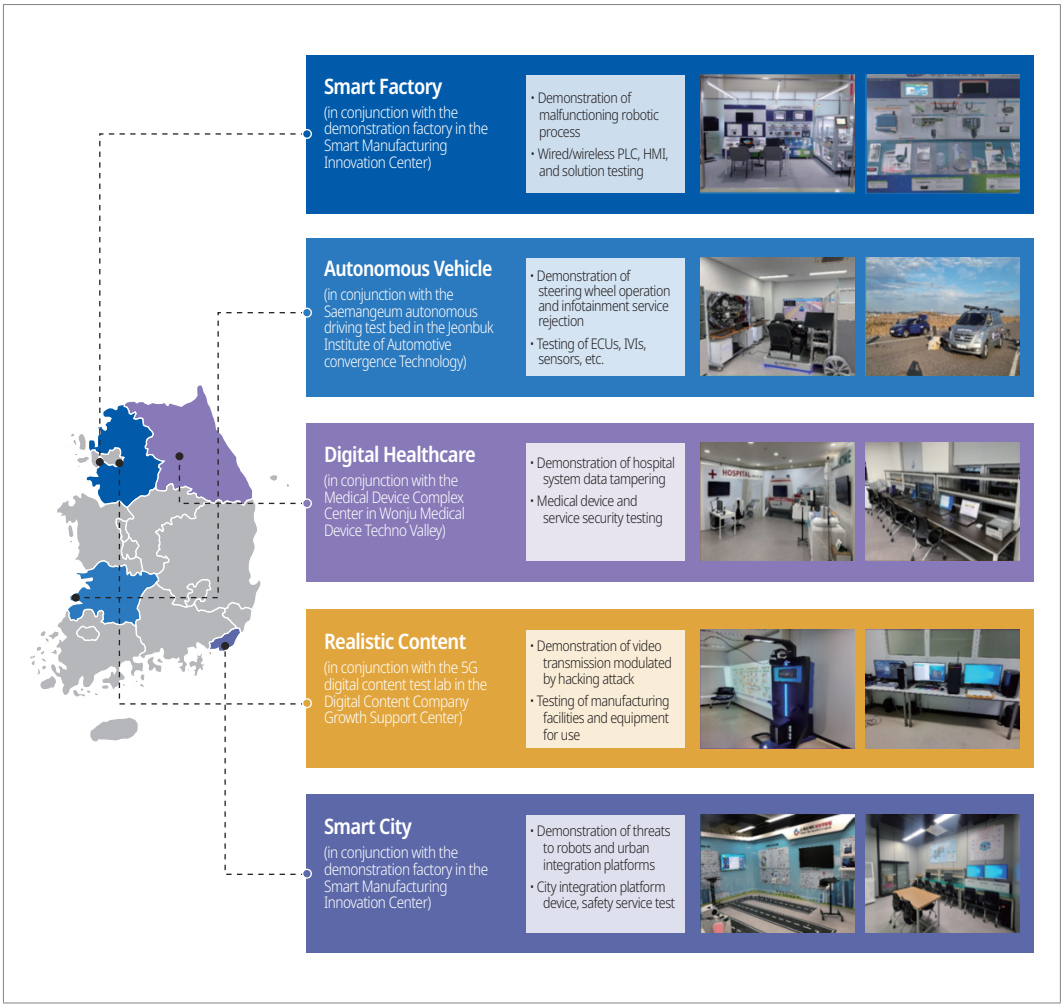
of Automotive convergence Technology (JIAT) in Gunsan city, Jeollabuk-do province. The test environment based on real-life automobile allows to support on discovering vulnerabilities in core devices such as automotive electronic control unit (ECU), and infotainment systems (IVI). Besides, the security test environment can be mobile in order to test autonomous driving sensors and V2X communications.

Digital healthcare-related Security Living Lab was implemented within the Medical Device Complex Center in Wonju Medical Device Techno Valley in Wonju city, Gangwon-do province. It is possible to demonstrate seven security threats, including a demonstration of data forgery in hospital systems and supports security tests through interworking between digital healthcare-related medical devices and services and medical information systems.

Realistic content-related Security Living Lab was built within the Digital Content Company Growth Support Center in Anyang, Gyeonggi-do. Here, it is possible to demonstrate the transmission of images that was corrupted by hacking attacks and test the security of production facilities, devices for use, and metaverse/digital twin services/devices.

Security Living Lab for smart city was built in the city of Busan to link with the national pilot smart city by the Dongnam Regional Information Security Center. Here, one can see simulation hacking scenarios for security threats of robot service and integrated platform-linked security threats. Furthermore, it is possible to test the security of integrated platform linkage, robot service, safety service, and smart city IoT devices.

Figure 2-4-5-2 Five major convergence service security living labs



Chapter 5

Financial Services

Section 1 Financial Service Security

1. Policy Changes by Time

A. Infrastructure Development (2000-2010)

During this period, the government established the foundation for financial security by proactively building a security infrastructure in both policy and technology aspects to prevent financial cybersecurity incidents with the launch of Internet banking services. In 2002, the government applied accredited certificates to electronic financial transactions for the first time in the world and established a financial Information Sharing and Analysis Center (ISAC).

In 2005, the Financial Supervisory Service in cooperation with the Financial Supervisory Commission announced the 'Comprehensive Measures for Enhancing Electronic Transaction Safety', applying measures such as the use of security programs to all financial sectors, and enacted the 「Electronic Financial Transactions Act」 in 2006, which is the basic law for financial security.

B. Improvement (2011-2014(1st Half))

In 2011, the Financial Services Commission (FSC) announced the 'Comprehensive Measures for Reinforcing IT Security for Financial Institutions', reinforcing the regulatory obligations on financial institutions, such as Chief Information Security Officer (CISO) mandate. In addition, the FSC established a department responsible for financial security, and as a follow-up measure for '3.20 cyber terror' in 2013, announced the 'Comprehensive Measures to Enhance Security for Financial Computing Systems' with an emphasis on reinforcement of financial companies' security management systems. These measures include separating financial computer networks and establishing Fraud Detection System (FDS) for financial companies.

When a credit card company's customer data breach occurred in 2014, a 'comprehensive measure to prevent the recurrence of personal information breach in the financial sector' was announced in cooperation with the relevant ministries. Accordingly, financial institutions' excessive collection and use of customer information were reformed by ensuring the right to informational self-determination of financial customers and by significantly raising sanctions against companies in case of an information breach.

C. Autonomous Security (2014(2nd Half)-2017)

As the financial security paradigm shifted to an autonomous security system with the facilitation of Fintech industry, the FSC announced the 'Finance and IT Convergence Support Plan' in January 2015 and reformed financial security regulations including minimizing ex-ante regulations, reflecting the principle of technological neutrality and clarifying who is responsible for financial cybersecurity incidents. Besides, the FSC presented detailed implementation tasks for self-security, such as strengthening self-inspection of financial companies and establishing a fraud information sharing system through 'Measures to Establish Autonomous Security System in Financial IT Sector' (June 2015). Meanwhile, the FSC had the Financial Security Institute play a role as a financial security professional organization that supports autonomous security by providing technical support for financial companies' own security evaluation and preparing security guides.

D. Digital Finance Innovation (2018-Present)

As the industrial structure began to change worldwide in 2018 due to the 4th Industrial Revolution, the FSC announced the 'Measures to facilitate Fintech innovation' (March 2018) and promoted facilitating Fintech, one of the 8 leading businesses of innovative growth. The FSC promoted the strengthening of the security support system and safety in the financial sector to respond to the potential risks of Fintech innovation through support for step-by-step security assessments and security consulting for innovative technologies, advancement of the information sharing system between the Financial Security Institute and financial companies for countermeasures against security incidents, and expansion of RegTech applications.

Furthermore, the FSC announced the 'Measures to expand the use of the financial cloud' (March 2018) and expanded the scope of use of the financial cloud to important information processing systems. Meanwhile, it is promoting cloud security, such as evaluating the safety and standards set up for using and providing cloud services, and strengthening supervision and inspection of cloud services according to the expansion of cloud use.

In 2020, as the need to strengthen the digital risk response system rises due to emerging technologies and the COVID-19 pandemic, the FSC announced the 'Comprehensive Innovation Plan for Digital Finance' in July 2020. The FSC is working on setting up a management and supervision framework for digital financial security to promote stability in digital finance and establishing a cyber-risk control framework that encompasses the public and private sectors.

In addition, the FSC is working on full revision of the 「Electronic Financial Transactions Act」 enacted in 2006 with the context of building a framework for digital finance user protection, rationalizing the non-face-to-face identification and authentication, reinforcing risk management on third-party due to financial IT outsourcing expansion, strengthening the Chief Financial Security Officers' authority, and establishing financial security governance framework.

In 2021, as non-face-to-face financial services accelerates due to the impact of COVID-19, the FSC is working on safe identification standards for non-face-to-face authentication so that financial users can verify their identity for non-face-to-face online financial services. The Commission is also working on financial infrastructure

development to support digital innovation using artificial intelligence. In order to bring diverse ideas into financial services, the FSC is planning to support to foster Fintech industry by introducing digital sandbox.

2. Policy

A. Policy Governance

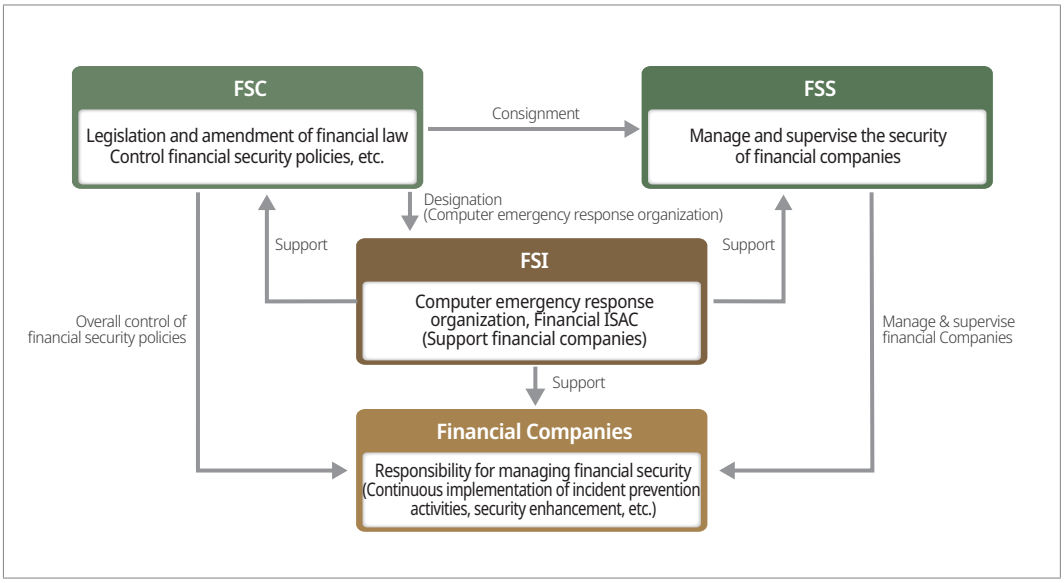
The Financial Services Commission (FSC) oversees and manages matters related to financial security policies and systems and supervision, inspection, and sanctions of financial companies in accordance with the 「Electronic Financial Transactions Act」 and the 「Credit Information Use and Protection Act」. The Commission is also responsible for the head office that coordinates cyber incident response, and charge of incident information collection/dissemination, alerts/warnings, and emergency response measures.

The Financial Supervisory Service manages and supervises the security management status of financial companies entrusted by the FSC according to the 「Electronic Financial Transactions Act」. If a violation of laws and regulations is identified through the supervision, the Financial Supervisory Service may recommend corrective orders, cautions, warnings, and reprimands to the FSC, and the FSC will review and take action. Moreover, being commissioned by the FSC, the Financial Supervisory Service conducts other electronic finance and security-related tasks, such as reviewing electronic finance business licenses and receiving IT plans and results of vulnerability assessments.

The Financial Security Institute is a computer emergency response organization under the 「Regulation on Supervision of Electronic Financial Transactions」, and also a financial ISAC under the 「Act on the Protection of Information and Communications Infrastructure」, and carrying out tasks to prevent and respond to cybersecurity incidents in the financial sector by establishing and operating a Financial Security Operations Center, sharing information on cyber threats and abnormal financial transactions, and assessing vulnerabilities in electronic financial infrastructure. In addition, the Financial Supervisory Service supports the establishment of an autonomous security system in the financial field, through support for the establishment of financial security policies by the FSC, inspections by the Financial

Supervisory Service, evaluation of self-security and conformance tests by financial companies, operation of financial security Regtech portal, development of financial security guides, and training of financial security experts.

Figure 2-5-1-1 Financial Security System



Recently, the following efforts are being made to strengthen security support for sustainable digital finance innovation: building an information-sharing system for voice phishing scams in the financial sector, efforts to strengthen cyber threat response capabilities of the financial sector, collecting and responding to dark web threat information, strengthening autonomous security capabilities for the introduction of new financial technologies such as support for verification of security for non-face-to-face personal identity verification, support for safe use of cloud computing services, support for vulnerability assessments such as open banking and financial regulation sandboxes, and support for policies and technologies related to AI in the financial sector.

As an entity in the financial sector's autonomous security system and the entity responsible for the security of its own financial services, financial companies carry out activities to prevent financial security incidents under the responsibility of the CEO. Also, they perform various activities to strengthen their own security capabilities such as securing financial security personnel and budgets. Recently, with the expansion of non-face-to-face financial services due to the digital transformation in the financial

industry, they are making an effort to establish and implement a digital financial risk response system.

B. Policy Summary

The Financial Services Commission (FSC) is constantly revising electronic financial security regulations to promote Fintech innovation and establish an autonomous security system in the financial sector. The FSC changed ex-ante regulations to ex-post regulations and revised mandatory security regulations that could be an obstacle to the entry into the Fintech industry, so that financial companies can reinforce cybersecurity and internal control on their own and establish a private-centered autonomous security system that meets the Fintech era. Furthermore, the Commission abolished procedural security regulations such as the certification method evaluation committee, the obligation to use nationally certified security products, and the pre-security evaluation system.

The FSC further expanded its support for establishing an autonomous security system for financial companies along with the reform of security regulations. It also reinforced the self-inspection of financial companies by supporting small and medium-sized financial companies that lack IT audit capabilities and strengthening the internal audit consultation system for financial companies in the IT sector. The Commission expanded the scope of service use, established guidelines and service standards, and strengthened the supervision and evaluation of cloud services together to facilitate the use of cloud services by financial companies. In addition, the FSC reorganized financial security-related guidelines so that financial companies can use them in a timely manner. The FSC also established a process for requesting a security review from the Financial Security Service so that financial companies can operate their own security review system with security expertise in new financial technologies.

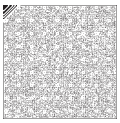
In accordance with the amendment of the 「Credit Information Use and Protection Act」 in February 2020, the FSC is promoting to deploy 'Routine Inspection of Personal Data Protection at Financial Institutions' and the 'Consent rating system for information utilization' in order to revitalize the data economy through safe data utilization. The FSC announced the 'Digital Finance Innovation Plan' in July 2020,. Also, it carries forward financial security measures such as establishing a digital financial security management and supervision system suitable for the post-COVID era, enhancing

financial security-related private governance that strengthens CISO authority and responsibility of the board of directors, and establishing a crisis management system in the financial sector that encompasses public and private sectors.

With the help of the government's facilitation of Fintech innovation and regulatory reform such as the close of mandatory use of accredited certificates, simple payment and simple remittance services using simple authentication methods have continuously increased. As of the first half of 2021, the average daily use of simple payment services was 559 billion KRW, and the average daily use of simple remittance services increased to 481.9 billion KRW. In addition, new Fintech services such as asset management, overseas remittance, financial crowdfunding, Robo-advisors, peer-to-peer (P2P) loans, and InsureTech are also being continually launched. Since the deployment of the financial regulation sandbox system in April 2019, a total of 185 innovative financial services have been designated for launching as of the end of 2021.

After the full implementation of open banking to promote financial innovation (2019), with 30 million net subscribers and 100 million net registered accounts in 2021, about 105% of the domestic economically active population (28.53 million, as of October 2021) is using open banking. The convergence of new technology and finance is being achieved through various regulatory exceptions such as comparison of online loan products, face recognition payment, and NFC payment service through the platform.

With the advancement of social engineering attack techniques such as malicious apps with phone number exploitation functions, related ministries jointly announced a 'Comprehensive Plan to Fight Voice Phishing' in June 2020 to establish a trust foundation for the digital economy. The government is reinforcing the following activities to prevent and respond to the damage of voice phishing, a crime infringing on people's livelihood: establishing a comprehensive response system to prevent the illegal use of communication means such as prepaid phones, establishing a system to filter out false indications of phone numbers (forgery) impersonating public institutions or financial companies, improving the procedure for canceling phone numbers using voice phishing, development of new technology to prevent voice phishing using big data and AI, establishing a joint financial consortium to advance the FDS (Fraud Detection System) of financial companies, strengthening publicity to prevent voice phishing, etc. In this regard, the government amended the 「Special Act on the Prevention of Loss caused by Telecommunications-based Financial Fraud and



Refund for Loss」and brought it into effect (November 20, 2020).

Revision of the Credit Information Use and Protection Act enabled MyData service providers to offer integrated management services to users on personal financial data by requesting transmission to the data subjects.

As AI technology is used in financial services, the FSC drafted up the model standards, 'Finance Services AI Guideline' to raise trust for the related services. The FSC also amended the 「Specific Financial Information Act」 to improve the transparency of virtual asset transactions and protect users, and established and implemented standards to restrict virtual asset transactions.

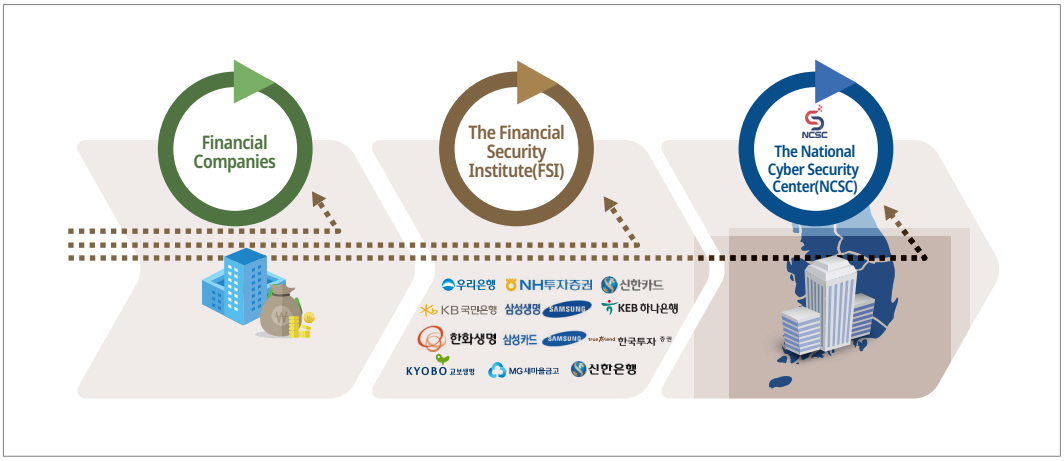
Section 2 Cyber Attack Response & Information Sharing in Financial Sector

1. Financial Security Operations Center

The Financial Security Institute (FSI) plays the role of the Financial Information Sharing and Analysis Center (ISAC) in accordance with the 「Act on the Protection of Information and Communications Infrastructure」 and the computer emergency response organization in accordance with 「Regulation on Supervision of Electronic Financial Activities」.

The FSI operates the Financial Security Operations Center to perform security control for the entire financial sector and raises the security level of the financial sector by establishing a triple-layered security operations system along with the security operations system performed by financial companies and the National Cyber Security Center.

Figure 2-5-2-1 Security operations system in financial sector



The Financial Security Operations Center detects and analyzes suspicious activities, develops and applies the latest detection techniques, shares information on cyber threats, etc.

Security incident detection and analysis is a task that detects and analyzes cyberattack attempts against financial companies 24 by 7 in real-time, using the financial security control system. In 2021, approximately 6.35 million incidents were detected and analyzed. Regarding intrusion attempts that are considered cyberattacks, measures are taken as immediately notifying financial companies to filter the attack attempts or to fix the vulnerabilities in the system. In 2021, ransom DDoS attacks targeting banks and zero-day attacks targeting Log4j vulnerabilities were detected and propagated to support the response of financial companies.

The development and application of the latest detection techniques are to apply to detection rules so that the financial security operations system can more effectively detect and analyze cyberattacks targeting the financial sector. Since 2019, AI-based intrusion detection methods have been applied to detect and respond to new intrusion threats. In order to increase the effectiveness of the detection techniques, the FSI is responding by collecting information on infringement activities through various channels while strengthening cooperation with national organizations such as the National Cyber Security Center.

Cyber threat information sharing refers to the FSI's prompt sharing of information

that needs an urgent response among the breach information detected by financial companies through mutual information exchange with financial companies, related organizations, and security companies. In 2021, about 2.52 million threats were shared. In addition, in order to contribute to strengthening security at the national level, the Financial Security Institute maintains close cooperation with financial authorities, e.g., the Financial Services Commission and the Financial Supervisory Service, and also with the National Cyber Security Center, the Prosecution Service, the Korean National Police Agency, and the Korea Internet & Security Agency.

Figure 2-5-2-2 Information sharing system on cyber threats

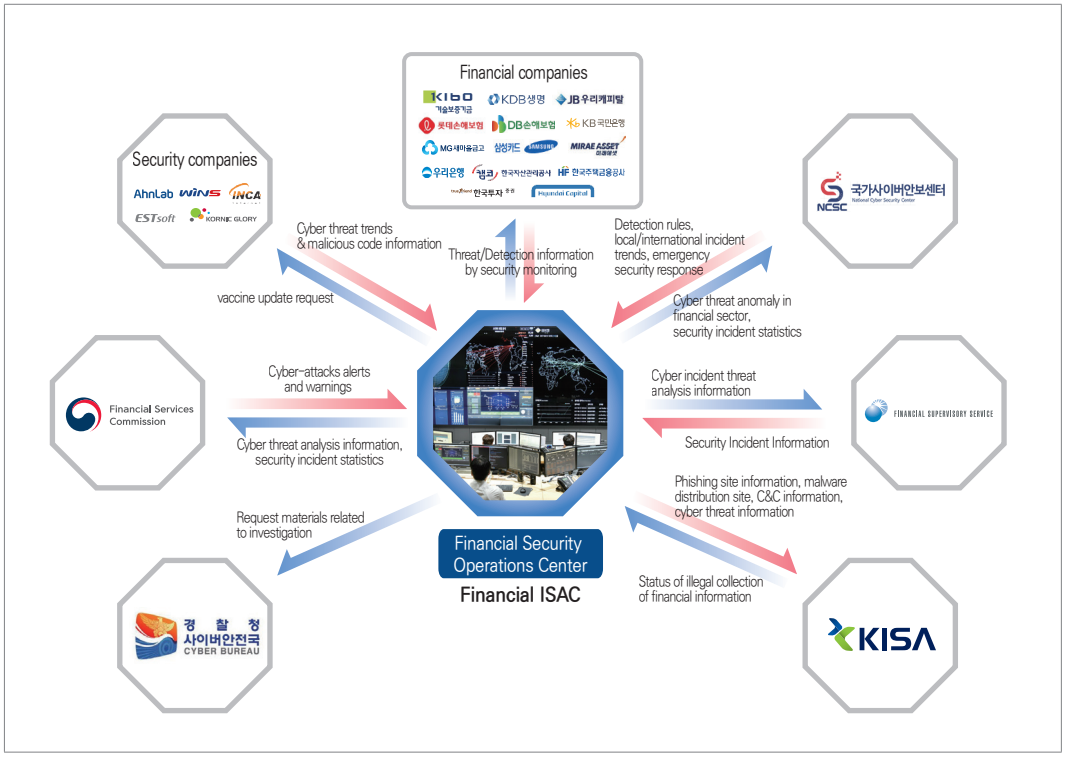
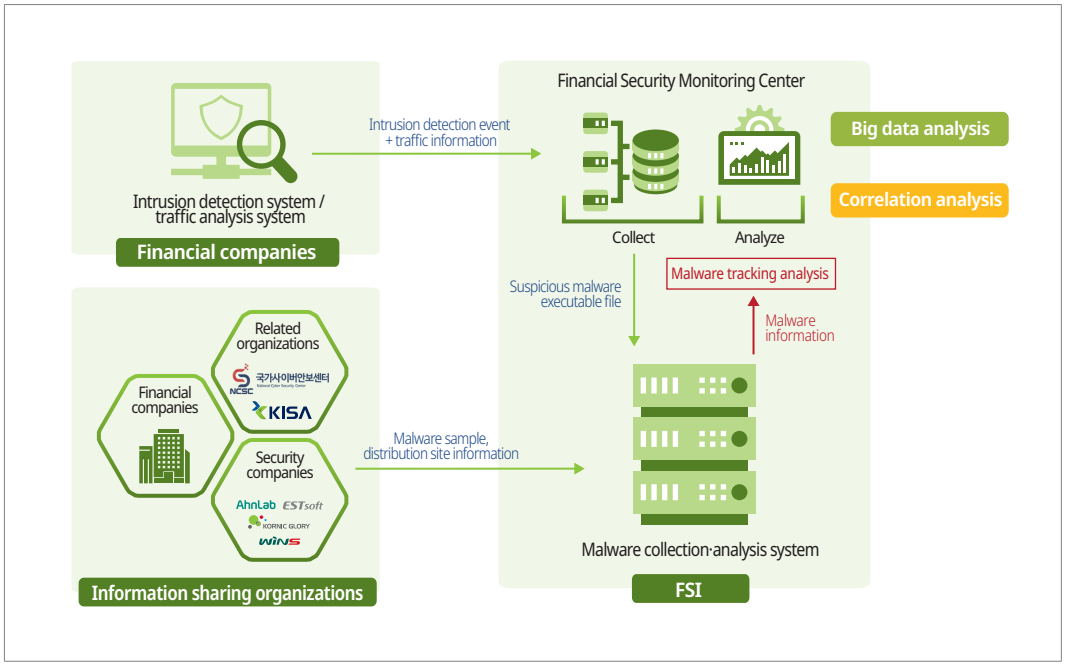


Figure 2-5-2-3 Financial Security Operations System

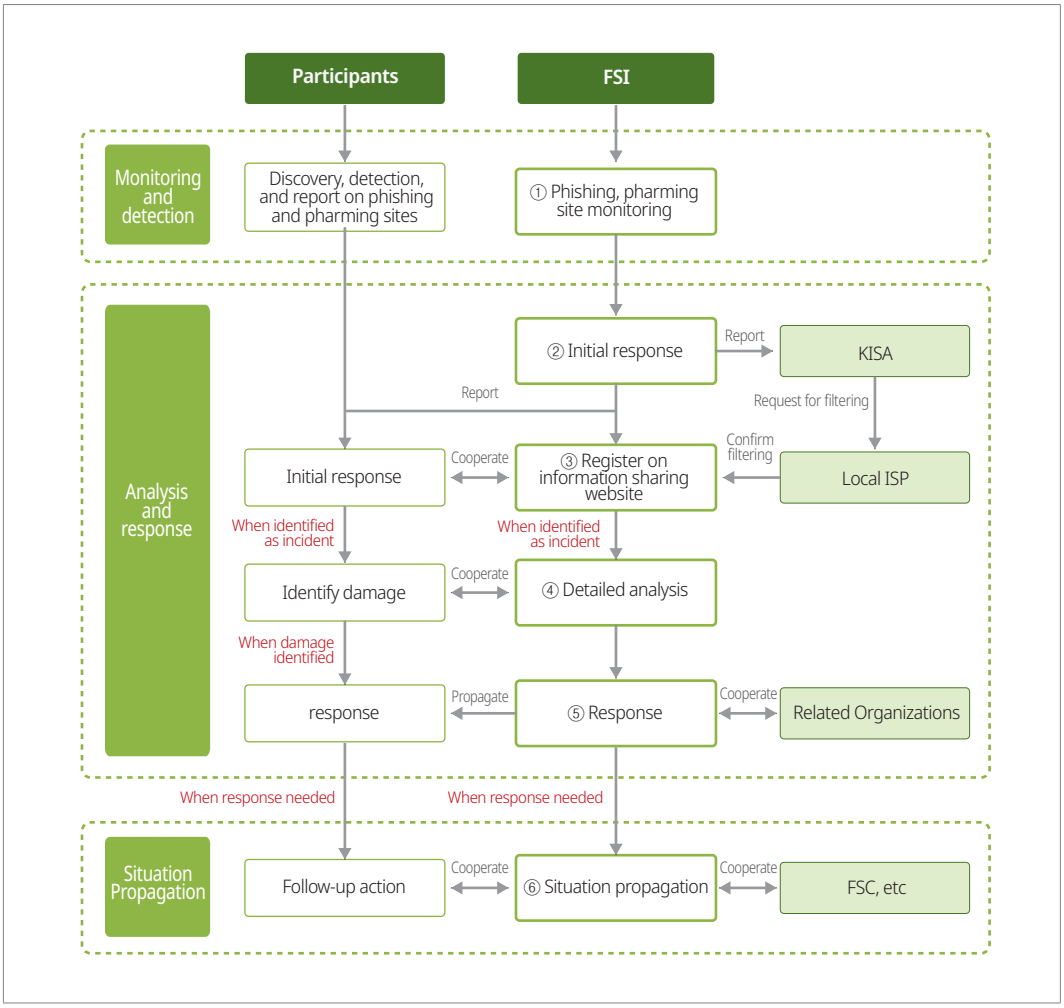


2. Phishing and pharming Monitoring

The Financial Security Institute (FSI) has developed and operated a phishing detection system to detect, analyze, and filter phishing and pharming sites on rogue financial companies' homepages to prevent the spread of fraud and potential damage to financial consumers.

First, the FSI detects and analyzes suspected phishing and pharming sites by the phishing detection system. If malicious behavior such as collecting personal information is detected, the site is reported to the Korea Internet & Security Agency and filtered through an Internet service provider (ISP). In addition, the information is registered on the information sharing website so that financial companies can take measures such as posting warning notices to customers.

Figure 2-5-2-4 Monitoring procedure of phishing and pharming sites



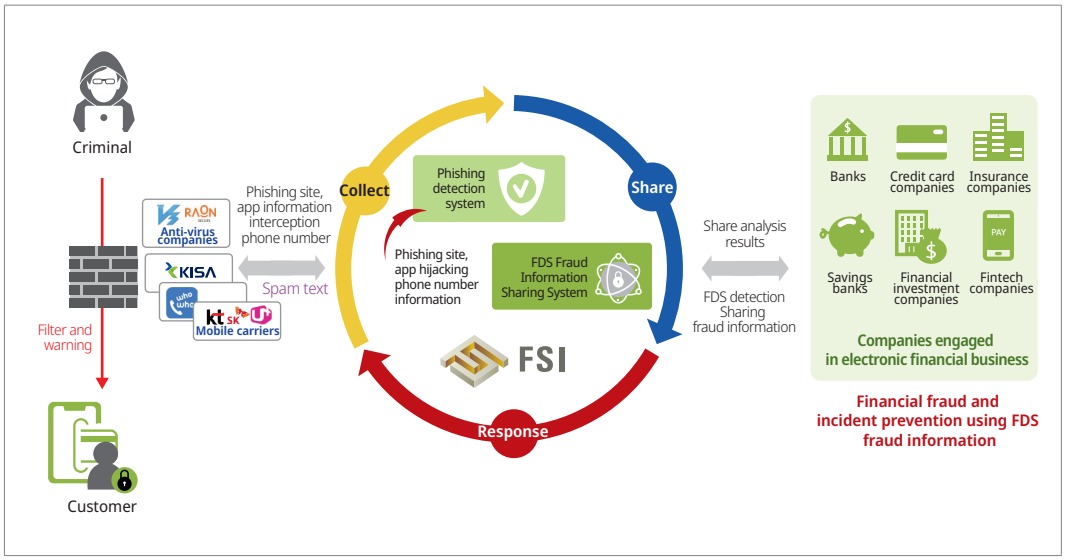
The FSI detected about 26,000 phishing and pharming attempts in 2021. Besides, it is estimated that damage to financial consumers of about 169 billion KRW was prevented based on the average amount of damage per case of phishing and pharming sites, which is about 6.5 million KRW, specified in the annual police statistics report of 2020 (published in December 2021). Meanwhile, since 2019, it has developed a function that detects the distribution of malicious voice phishing apps and applied it to the phishing detection system, thereby taking a preemptive response to phishing and pharming as well as to the mobile domain of voice phishing.

3. Prevention and response to voice phishing

To implement the 'Comprehensive Plan to Eliminate Voice Phishing (June 2020) prepared by the FSC in 2020 to respond to voice phishing, the FSI, along with commercial banks and large electronic financial companies, prepared technical measures that can be applied to the entire financial sector, including analysis of voice phishing trends and cases, and research on new voice phishing techniques blocking technology.

In January 2021, the FSI established a 'Sector-wide Voice Phishing Information Sharing System' to operate a systematic cooperative system for collecting, sharing, and responding to the voice phishing information at the level of the financial, public, communication, and security sectors. After the system's full-fledged operation, it supported sharing and response to 22,000 cases of voice phishing information in 2021.

Figure 2-5-2-5 Sector-wide Voice Phishing Information Sharing System



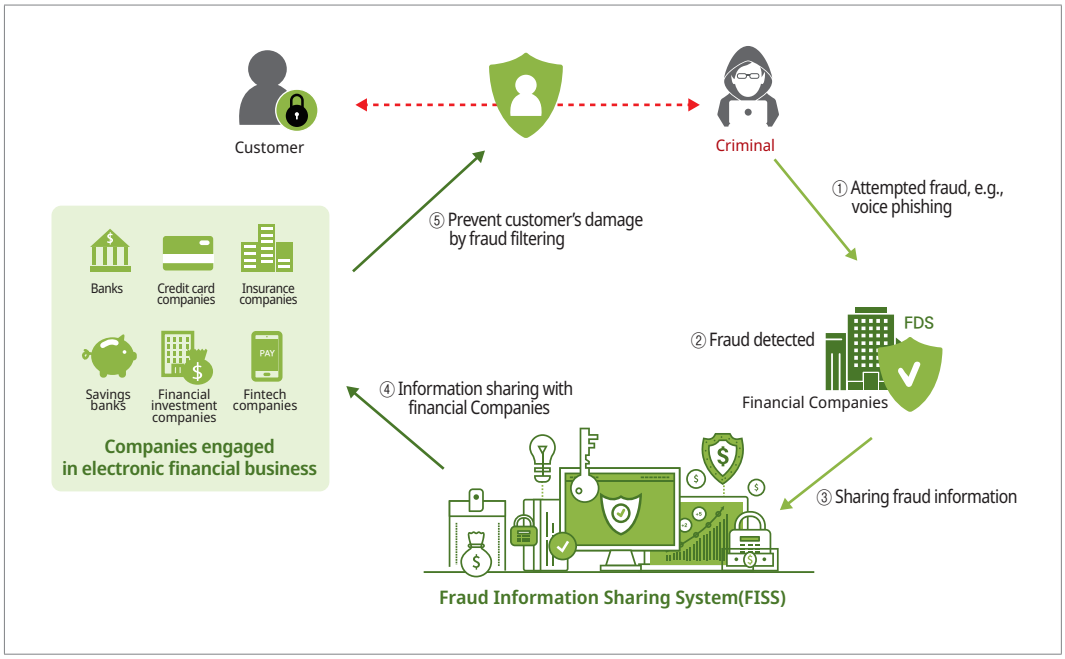
4. Fraud Information Sharing

As attacks against financial consumers such as voice phishing and electronic financial fraud that abuse social engineering attack techniques and tricks are becoming more sophisticated and intelligent, each financial company has established

and operated a FDS to protect financial consumers' assets. In order to allow the financial sector to jointly respond to financial fraud, since February 2016, the FSI has established a Fraud Information Sharing System (FISS) that shares fraud information detected by each financial company's FDS.

In 2021, 90 financial companies and electronic financial companies participated in sharing fraud information, and by sharing 156 fraud information, approximately 9.76 billion KRW in damage to financial consumers was prevented.

Figure 2-5-2-6 **Fraud Information Sharing System**



5. Malware collection, analysis and response

The FSI collects malicious code that may affect the financial sector through various channels. It also operates a malicious code analysis system, which analyzes and profiles (correlation and grouping) malicious code that is becoming more intelligent such as in ransomware and APT attacks. After analysis, information on identifying threat groups and pattern tracking/observation is provided to financial and related organizations. In addition, information such as attempts to infect the system of financial companies, malicious code, and websites distributed for financial fraud purposes are also shared

with financial companies and related organizations. In 2020, the Financial Security Institute established a next-generation malicious code analysis system. In 2021, the Financial Security Institute expanded the system's scope, upgraded the malicious code detection function by utilizing the latest analysis technology and artificial intelligence technology, and improved the function to enable efficient analysis of malicious codes not detected based on signatures.

The number of malicious code collected and analyzed in 2021 was about 24,260,000, of which about 102,500 cases identified as actual malicious code were shared with financial companies and related organizations.

Furthermore, the FSI is researching cyber threat intelligence through profiling of threat groups targeting Korea. In 2021, the FSI published reports on 'Analysis of Major Encryption Algorithms Used by Ransomware', 'Analysis of Cyberattack Threats Targeting Credit Card Information', 'Profiling of Organizations Distributing Malicious Voice Phishing Apps'.

6. Security incident response & recovery drill

Financial companies and electronic financial business operators conduct security incident response and recovery training at least once a year in accordance with the 「Regulation on Supervision of Electronic Financial Activities」 in order to reinforce their ability to respond to and recover from various types of cybersecurity incidents.

The FSI supports the training of financial companies using self-developed training content in response to security incidents such as DDoS attacks, infrastructure hacking attacks, and APT attacks. In 2021, a total of 535 security incident response drills were conducted.

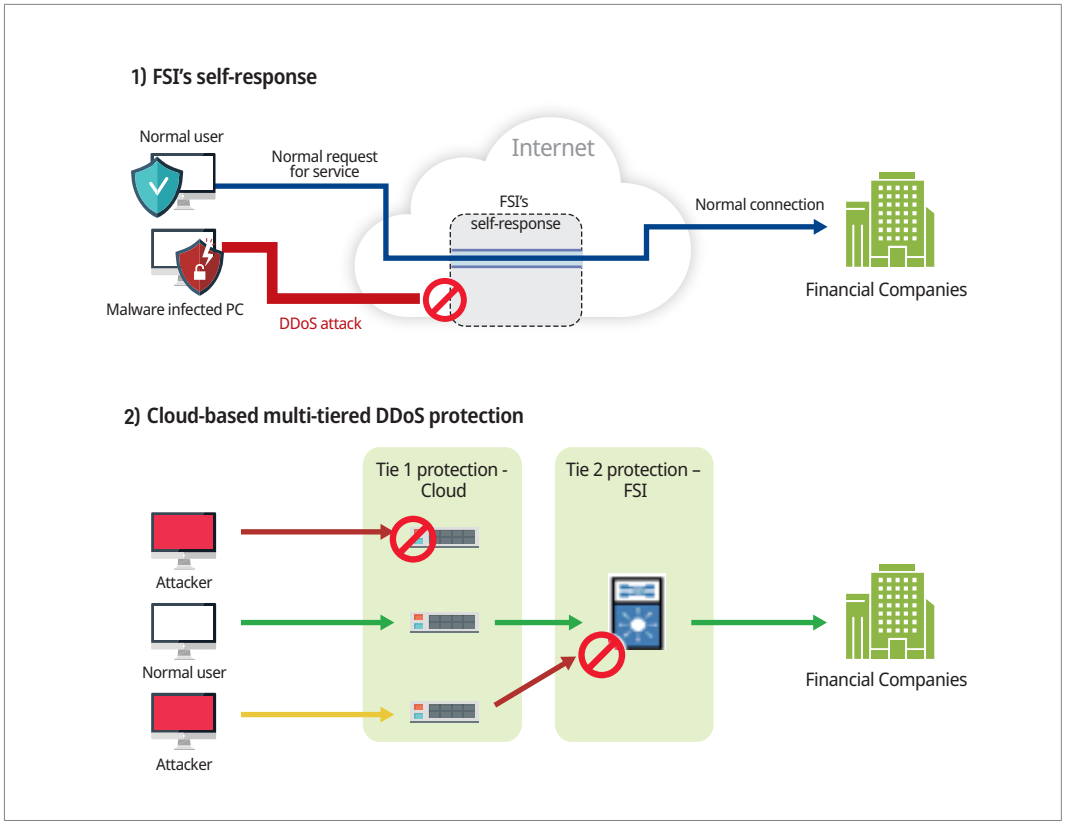
7. DDoS attack response

Financial companies are responding to DDoS attacks by establishing their own cybersecurity system to prevent cybersecurity incidents in accordance with Article 15 of the 「Regulation on Supervision of Electronic Financial Activities」. In the event of a DDoS attack that exceeds the ability of a financial company to respond, the Financial Security Institute operates a DDoS attack emergency response center and mitigates

DDoS attacks by redirecting DDoS traffic to the large-capacity cloud.

Moreover, the FSI has established a close information sharing system with the National Cyber Security Center, the Korea Internet & Security Agency, the Korean National Police Agency, carriers, security vendors, and related organizations abroad to respond effectively against DDoS attacks.

Figure 2-5-2-7 **Response system of DDos Emergency Response Center**



Section 3

Security Evaluation/Inspection on Financial IT/ Electronic Finance & Fintech

1. Vulnerability assessment

As a computer emergency response organization pursuant to the 「Regulation on Supervision of Electronic Financial Activities」 and a Financial Information Sharing and Analysis Center (ISAC) pursuant to the 「Act on the Protection of Information and Communications Infrastructure」, the Financial Security Institute (FSI) conducts security vulnerability assessments on electronic financial infrastructure and major information and communications infrastructure in the financial sector.

The FSI uses the latest assessment items and technology to assess security vulnerabilities in a total of 10 areas, including information security management systems and penetration tests, for information processing systems and information communication networks used in electronic financial transactions.

The assessment items are based on the 「Vulnerability Evaluation Criteria for Electronic Financial Infrastructures' Security」 by the FSI and the 「Vulnerability Analysis/Evaluation Criteria for Major Information and Communication Infrastructure」 by the Ministry of Science and ICT (MSIT).

In 2021, a new evaluation standard was established for the evaluation of the cloud system that was built and operated by financial companies, and a theme check* was performed for open banking mobile applications in each financial sector.

* This selects issues related to the latest security threats in the financial sector and areas of concern for electronic infringements and provides annual vulnerability inspection services to employee organizations.

Table 2-5-3-1 **Major evaluation contents by field of security vulnerability evaluation**

Evaluation field		Main Content	Method
Infrastructure area	Information protection management system	• Evaluating the adequacy of internal regulations and procedures of financial companies, focusing on the Electronic Financial Transactions Act and Regulation on Supervision of Electronic Financial Activities	Checklist-based assessment, Using automation tools, Manual assessment, Interview with the person in charge, On-site assessment, etc.
	Server	• Technology-oriented assessment of the adequacy of operating system security settings, such as activation of unnecessary services when operating information processing systems	
	Database	• Technology-oriented assessment of the adequacy of security settings for DBA account privileges, passwords, etc.	
	Network infrastructure	• Management-centered assessment of the adequacy of network configuration and availability, such as network separation and network access control	
	Network equipment	• Technology-oriented assessment of the adequacy of security settings for network operation equipment	
	Information protection system equipment	• Technology-oriented assessment of the adequacy of security policy and information protection system security settings, etc.	
Service area	Web application	• Technology-oriented assessment of the possibility of infringement on web-based electronic financial transaction services such as internet banking	
	Mobile application	• Technology-oriented assessment of the possibility of security breaches for mobile-based electronic financial transaction services such as mobile banking	
	HTS	• Technology-oriented evaluation of the possibility of infringement on HTS applications provided by securities companies	
Common area	Penetration testing	• Assessment of the possibility of internal penetration using various vulnerabilities and the risk of leakage of important information such as personal credit information	Scenario based assessment

2. Security evaluation on cloud computing service providers

When using commercial cloud computing services, financial companies and electronic financial business operators must perform security evaluations on cloud computing service providers (CSP), while the Financial Security Institute (FSI) has supported financial companies' CSP security evaluations as a computer emergency response organization from 2019. With the introduction of the joint evaluation method

in 2021, the burden of CSP security evaluation has been alleviated by preventing the overlapping evaluation of the same CSP operator's cloud service by financial companies.

When evaluating the safety of CSPs, the FSI evaluates 'Basic security measures', which are general security standards that CSPs must comply with, along with 'Additional security measures for the Financial Sector', which are specialized standards in the financial sector. In 2021, the FSI supported the evaluation of the stability of financial companies' CSPs for 7 CSP operators and 9 cloud services (175 cases).

Also, the FSI established an 'integrated support system for CSP safety evaluation' that can share CSP safety evaluation-related information and evaluation results with financial companies. In this way, the FSI is contributing to the creation of an ecosystem for cloud use in the financial sector and the enhancement of security.

3. Joint inspection of subsidiary electronic financial businesses

Financial companies must conduct vulnerability assessments on the information processing systems of subsidiary electronic financial business operators linked to information technology. In order to support this, the FSI has formed a joint assessment team with financial companies to conduct vulnerability assessments.

In 2021, the FSI developed a 'Guideline for Security Vulnerability Inspection of Subsidiary Electronic Financial Business Operators' and conducted security vulnerabilities checks on 38 CD VAN, card VAN, and CMS subsidiary electronic financial business operators jointly with financial companies.

Furthermore, the FSI is proactively responding to third-party risks by establishing the 'Integrated Support System for Subsidiary Electronic Financial Business Operators' that can jointly inspect security vulnerabilities with financial companies and conduct integrated management of inspection results and contract relationships.

4. Joint inspection of personal (credit) information trustees

The financial company (the truster) shall periodically manage and supervise whether the trustee who performs the management affairs of personal information handles

the personal (credit) information safely. Through the joint inspection method, once a year, the FSI checks the adequacy of technical and administrative protective measures necessary to ensure safety when trustees handle personal (credit) information.

In 2021, the FSI provided a guide for trustees' self-inspection and practical measures to ensure the safety of personal (credit) information and conducted inspections for a total of 100 trustees according to requests from 70 employee organizations.

Meanwhile, the FSI has established and operated the 'personal (credit) information trustee inspection support system' to efficiently conduct inspections of trustees in the financial sector.

5. Fintech vulnerability assessments

The FSI conducts vulnerability assessments on Fintech companies and online investment-linked financial businesses participating in open banking and financial regulation testbeds (innovative financial services, etc.) to create a safe open banking environment and to ensure the reliability of innovative Fintech services.

There are two types of Fintech vulnerability assessments. The first one is the 'Fintech company vulnerability assessment' that examines whether a Fintech company has established a security management system and operated its system based on it. The other one is the 'Fintech service vulnerability assessment' that checks Fintech services (web/mobile) for vulnerabilities.

The FSI conducted a total of 244 vulnerability assessments for Fintech companies in 2021.

Part 3

Create Cybersecurity Environment

Chapter 1

Cybersecurity Industry

Section 1 Overview

The government established the 「K-ICT Security Development Strategy」 and enacted the 「Act on the Promotion of Information Security Industry」 (hereinafter, 'Act on the Information Security Industry') in 2015. In 2016, the government announced the '1st Information Security Industry Promotion Plan'. This Plan sets out goals for Ministries to promote cybersecurity start-ups, expand cybersecurity investment and global market, and create an ecosystem for ICT convergence industry growth.

In accordance with the enactment of the 「Act on the Information Security Industry」, in terms of the demand side, the government strengthened the virtuous cycle of industrial ecosystem by creating a cybersecurity market. On the supply side, the government created regulations for the systematic promotion of the cybersecurity industry and laid the foundation for fostering and strengthening the domestic cybersecurity industry as a key component of the cyberattack response system.

The foundations for cybersecurity industry growth are laid by 「Act on Information Security Industry」. In 2017, the government strived to create an ecosystem for the cybersecurity industry to facilitate the competitiveness of security companies. It

includes the disclosure system of information security and fostering convergence security workforce, creating a performance assessment system foundation, establishing the guidelines, explanatory meetings for the regulations, enterprises' self-disclosure, and developing product performance assessment guidelines.

Following the 「Act on the Information Security Industry」, in 2017, the government established the disclosure system of information security, laid the foundation for the performance evaluation system, and developed convergence security-related personnel training and security guides. The government also made efforts to lay the foundation for the information security industry and to strengthen corporate competitiveness, such as through briefing sessions on the information security system, enterprises' self-disclosure, and the establishment and implementation of product performance assessment guidelines.

The National Security Office announced the 'National Cybersecurity Strategy' in April 2019. One of the goals of this strategy is to build foundations for the cybersecurity industry, and the government supports the growth of the cybersecurity industry. In addition, the National Security Office formulated the 'National Cybersecurity Basic Plan' in September 2019 and developed and implemented this strategy with the relevant ministries.

In 2020, the spread of non-face-to-face services caused by the COVID-19 pandemic has accelerated the movement toward digital transformation. To strengthen the resilience of cybersecurity in the private sector and create safe cyberspace, the MSIT announced the '2nd Information Security Industry Promotion Plan (2021-2025)' in June 2020.

The plan aims to raise total cybersecurity sales to 20 trillion KRW, nurture 100 companies with more than 30 billion KRW in sales, and train 165,000 cybersecurity personnel by 2025. To achieve this plan, it was necessary to strengthen the autonomous cybersecurity capabilities for SMEs, strengthen a win-win cooperation system between cybersecurity companies and develop next-generation security technologies, and build a positive cycle for personnel development management system. Accordingly, creating a new cybersecurity market through digital transformation, expanding private sector investment for cybersecurity resilience, and building a sustainable cybersecurity ecosystem were set as priority tasks.

In 2021, the importance of non-face-to-face service security was highlighted as non-face-to-face environments such as telecommuting and remote work and online classes spread rapidly due to the post-COVID-19 pandemic. Since the scope of the cybersecurity industry has been expanded to ICT security according to wired and wireless network connections such as home appliances, mobile devices, and industrial machines, the importance of cybersecurity has been emphasized more than ever. In response to these circumstances, the government supported the commercialization of secure non-face-to-face services that applied security technology to the services such as remote education, telecommuting, and non-face-to-face treatment so that safe non-face-to-face services could be provided promptly. The government also provided AI learning data based on disasters and biometric information, laying the foundation for a new domestic cybersecurity market.

As the convergence of traditional industries and ICT has accelerated, many experts have predicted the growth of the convergence security market for embedded security of smart factories and smart cars. In order to respond to this, the Ministry of Science and ICT (MSIT) announced the 'Strategic Plan to Foster Cybersecurity Industry' in February 2022. According to this strategic plan, the cybersecurity industry plans to take a leap forward as a next-generation strategic industry centering on the following four strategies: creating a new cybersecurity market, fostering a global first-class cybersecurity enterprises, expanding the ecosystem to strengthen the foundation of the cybersecurity industry, and secure the competitiveness of next-generation cybersecurity technology.

Based on the five-year comprehensive plan, the government plans to continuously promote the following methods so that the cybersecurity industry can continue to grow in line with the rapidly changing market by strengthening support for the convergence security industry, expanding secure non-face-to-face services, early settlement of cybersecurity disclosure system, reinforcing export assistance for cybersecurity companies, and fostering next generation talented workforce.

Section 2 Cybersecurity Markets

The Korea Information Security Industry Association surveyed the 1,283 domestic information security companies, and the followings are from the '2021 Survey of Information Security Industry'.

1. Cybersecurity Vendors

The survey identified that 655 companies have less than 20 employees (51.1%), 491 companies have between 20 and 100 employees (38.3%), 70 companies have between 100 and 200 employees (5.5%), and 67 companies have more than 200 employees (5.2%). Companies with less than 100 employees accounted for 85.7% of information security and 91.9% of physical security, accounting for 89.4% of the total.

Table 3-1-2-1 Number of employees of cybersecurity companies

(Unit of measurement: unit, %)

	Information Security		Physical Security		Total	
	Number of companies	Ratio	Number of companies	Ratio	Number of companies	Ratio
Less than 20 people	218	41.1	437	58.1	655	51.1
20 to 100 people	237	44.6	254	33.8	491	38.3
100 to 200 people	43	8.1	27	3.6	70	5.5
More than 200 people	33	6.2	34	4.5	67	5.2
Total	531	100.0	752	100.0	1,283	100.0

2. Cybersecurity market

The total sales of the cybersecurity industry in 2020 reached 12,224,252 million KRW, increased by 9.3% compared to that of 2019. Information security sales is increased by 8.0% from 3,618,773 million KRW in 2019 to 3,921,387 million KRW in 2020, and physical security sales is increased by 9.8% from 7,561,734 million KRW in 2019 to 8,302,865 million KRW in 2020.

Table 3-1-2-2 Sales status of the cybersecurity industry

(Unit of measurement: million KRW, %)

	Information Security		Physical Security		Total	
	2019	2020	2019	2020	2019	2020
Sales	3,618,773	3,921,387	7,561,734	8,302,865	11,180,507	12,224,252
Growth Rate	8.4		9.8		9.3	

Sales in the cybersecurity industry show an average annual increase of 9.1%, starting from 7,255,317 million KRW in 2014. Information security sales are annually increased by 14.5% on average from 1,735,865 million KRW, and physical security sales are annually increased by 5.8% on average from 5,519,452 million KRW. The continued increase in cybersecurity industry sales is mainly by the government regulations, awareness raised by increasing incidents, expanded cybersecurity investment, and efforts to discover the global market.

Table 3-1-2-3 Sales trends of the cybersecurity industry

(Unit of measurement: million KRW, %)

Year	Information Security	Physical Security	Total
2014	1,735,865	5,519,452	7,255,317
2015	2,108,659	6,110,086	8,218,745
2016	2,454,024	6,588,787	9,042,811
2017	2,744,940	6,840,822	9,585,762
2018	3,082,926	7,034,918	10,117,844
2019	3,618,773	7,561,734	11,180,507
2020	3,921,387	8,302,865	12,224,252
CAGR(2014 ~ 2020)	14.5	7.0	9.1

3. Exports

Total cybersecurity industry exports were 1,913,523 million KRW in 2020 increased by 8.8% from 1,779,846 million KRW in 2019. Information security exports in 2020 are expected to reach 145,592 million KRW, which went up by 19.5% from 122,766 million KRW in 2019. Physical security exports in 2020 are expected to reach 1,767,931 million KRW, went up by 6.7% from 1,657,080 million in 2019.

Table 3-1-2-4 Exports of the cybersecurity industry

(Unit of measurement: million KRW, %)

	Information Security		Physical Security		Total	
	2019	2020	2019	2020	2019	2020
Exports	122,766	145,592	1,657,080	1,767,931	1,779,846	1,913,523
Increase rate	18.6		6.7		7.5	

The exports are growing at an average annual rate of 3.8%, starting from 1,527,450 million KRW in 2014. Exports of information security are annually increased by 12.2% on average from 72,989 million KRW in 2014, and exports of physical security are annually increased by 3.3% on average from 1,454,461 million KRW in 2014.

Table 3-1-2-5 Export trends in cybersecurity industry

(Unit of measurement: million KRW, %)

Year	Information Security	Physical Security	Total
2014	72,989	1,454,461	1,527,450
2015	78,133	1,545,540	1,623,673
2016	88,978	1,400,102	1,489,080
2017	94,398	1,475,755	1,570,153
2018	82,363	1,473,769	1,556,132
2019	122,766	1,657,080	1,779,846
2020	145,592	1,767,931	1,913,523
CAGR(2014~2020)	12.2	3.3	3.8

Section 3 Cybersecurity Industry Regulations

1. Designation of specialized cybersecurity service company

A. Overview

The specialized cybersecurity company system refers to the designation of a specialized cybersecurity consulting company in accordance with the 「Information and

Communication Technology Industry Promotion Act」(hereinafter referred to as the 「Act on the Information Security Industry」). In order to facilitate quality vulnerability assessment and protection consulting services for critical infrastructure, this system has been implemented since 2001 to provide high-quality cyber security services by designating private companies with professional competence and credibility. This has been implemented in accordance with the 「 Act on the Protection of Information and Communications Infrastructure 」 and the 「 Act on the Information Security Industry」, and the relevant notices set out the details of designation criteria, procedures, methods, etc.

As highly skilled and resourced cyber threats increase, the government expands critical information and communication infrastructure designation. Along with this, the biennial vulnerability assessment is shortened to an annual process. To harbor the expansion, the Ministry of Science, ICT and Future Planning (currently the Ministry of Science and ICT (MSIT) revised the relevant laws in 2013 and developed the plan to improve the quality of services and facilitate the market through a system reform and additional designation of cybersecurity service companies.

The government held a public hearing to improve the designation process of specialized cybersecurity consulting firms in September 2012. It published the revised 「Information and Communications Technology Industry Promotion Act」 having enacted in February 2013. The law is now under the 「Act on the Information Security Industry」. The revision of the 「Notice on Designation of enterprises specializing in Security」 has eased the designation requirements for cybersecurity companies to facilitate the market and lowered the bars for new companies. After that, the name of the system and administrative department have been changed to 'Specialized Cybersecurity Service Company', and it has been revised and implemented since October 2017 to reflect the contents of post-management regulations.

Since October 2017, the MSIT has allowed companies that fulfilled the requirement to apply to the program at any time.

Table 3-1-3-1 Standard Criteria for designation of Specialized Cybersecurity Service Companies

Standard Criteria	Before revision	After revision (enforced on 20 May 2013)
Human Resources requirements	15 or more technical human resources (including 5+ high-level human resources)	10 or more technical human resources (including 3+ high or special level human resources)
Capital requirements	More than 2 billion KRW for paid-in capital	More than 1 billion KRW for total capital
Facility requirements	Possession of facilities and tools to carry out or support consulting activities	No change
Security requirements	Retention and compliance of information security management regulation	No change
Performance requirements	70 points or more based on work performance evaluation Metric evaluation: experience, specialization, reliability, and result of technology development (70 points) Non-metric evaluation: comprehensive examination (30 points)	70 points or more based on work performance evaluation Metric evaluation: experience, specialization, reliability, and result of technology development (85 points) Non-metric evaluation: comprehensive examination (15 points)

[Source: 「Act on the Promotion of Information Security Industry」Enforcement Rule Article 8, Ministry of Science and ICT Notification 2017-24 (attached Table 2)]

Designated cybersecurity service companies must be evaluated and strictly managed as their services to critical information and communication infrastructures affects national security, people's lives, and economic stability. Each year, the MSIT confirms that the designated companies comply with the requirements and obligations of laws and regulations.

In accordance with Article 23 (6) of the 「 Act on the Information Security Industry」, the government may annul the designation and suspend its business for a period of up to three months when it falls short of the requirements. It includes wrongful designation, operational failure, and misuse of the information acquired by the business.

The designated companies must report any critical changes by document within a month to the MSIT such as the changes in the chief executive officer, executive staff, paid-in capital, technical staff, and cybersecurity service management rules.

B. Designations

The government designated thirteen companies in total, nine in 2001, four in 2002. However, it revoked the designation for six companies. It designated eleven new

companies in 2014. Since October 2017, regular designation has started, and as of December 2021, there are 28 specialized companies.

Table 3-1-3-2 Specialized cybersecurity service companies

	Company Name	Designated Date
1	SECUI Corporation	November 29, 2001
2	AHNLAB, Inc.	November 29, 2001
3	A3SECURITY, Inc.	November 29, 2001
4	CYBER ONE, Inc.	November 29, 2001
5	ADTCaps, Inc.	October 8, 2002
6	SOMANSA, Inc.	March 28, 2014
7	CAS, Inc.	March 28, 2014
8	SSR, Inc.	March 28, 2014
9	WINS Co., LTD	March 28, 2014
10	IGLOO SECURITY, Inc.	March 28, 2014
11	SECURE ONE, Inc.	March 28, 2014
12	KEPCO KDN Co., Ltd.	March 28, 2014
13	FASOO Co., Ltd.	June 2, 2016
14	ENSECURE, Inc.	December 26, 2017
15	LOTTE DATA COMMUNICATION COMPANY	April 24, 2018
16	PIOLINK, Inc.	April 24, 2018
17	SHINHAN DS, Inc.	April 24, 2018
18	KTIS, Inc.	April 24, 2018
19	F1SECURITY, Inc.	May 16, 2019
20	KCA Corp.	July 22, 2019
21	KISCA company	February 24, 2020
22	SEEDGEN Corp.	July 29, 2020
23	RaonWhiteHat Corp.	July 29, 2020
24	HANSECURITY, Inc.	October 6, 2020
25	MobyDick, Inc.	November 10, 2020
26	SECURITY HUB, Inc.	December 29, 2020
27	LNJ TECH, Corp.	December 29, 2020

2. Designation of Specialized Network Security Monitoring Companies

A. Overview

In April 2010, 「Regulations on Management of Cyber Security Affairs」 stipulated establishing network security monitoring centers in national and public organizations to protect major countries' information systems from new types of cyberattacks like DDoS. Furthermore, in December 2010, the government listened to the opinions of the network security monitoring companies and announced the 「Notice on the designation of specialized network security monitoring companies」 to designate a professional company to operate a network security monitoring center.

In May 2013, the 「Regulations on Management of Cyber Security Affairs」 was established and revised for the designation and management of specialized network security monitoring companies in consultation with the Minister of Science and ICT and the NIS Director. In November 2016, the government changed the name to specialized network security monitoring companies. Moreover, in October 2017, the government revised the 「Notice on the Designation of Specialized Network Security Monitoring Companies」 to reflect the change in the name of the department. Moreover, in August 2019, the government revised the law by adding a section to provide the transfer and merger of specialized network security monitoring companies.

In order to be designated as a specialized network security monitoring company, a company must have at least 15 technical personnel and KRW 2 billion of equity capital, and pass the performance evaluation of work security monitoring. The detailed criteria for designation are as follows.

Table 3-1-3-3 Criteria for the designation of a specialized network security monitoring company

Examination Criteria	Conditions	Criterion
Manpower Requirements	15 or more technical personnel (High-level personnel: 3 or more; intermediate level personnel: 6 or more)	Conditions are met
Capital Requirements	More than 2 billion won in equity capital	Conditions are met
Performance Requirements	Pass the performance evaluation of network security monitoring	More than 70 points

[Source: Notice on the designation of specialized network security monitoring companies (Ministry of Science and ICT Announcement 2019-441)]

Table 3-1-3-4 **Standards for performance evaluation of network security monitoring**

Evaluation Criteria	Conditions
Experience (45 points)	Performance of the network security monitoring over the past year (preferential treatment for high proportion of self-employed people and dispatch monitoring)
Exportise (40 points)	Number of high-level technical personnel, methodology of network security monitoring, appropriateness of operating its own network security monitoring center, etc.
Reliability(15 points)	Corporate credit rating, information security certification company status, etc.
Other (optional)	Preferential treatment for venture companies, points deduction for experience in restriction on participation in bidding for public institutions

[Source: Notice on the designation of security system specialized companies (Ministry of Science and ICT Announcement 2019-441)]

There are almost no entry obstacles for specialized network security monitoring companies since the government minimized the designation requirements as long as they are met. It is to promote the competition for high-quality network security monitoring services. However, the government is strengthening the follow-up management in the public sector considering that its scale of damage is larger and wider than that of the private sector. The government annually examines the designated companies, and it could cancel the license if it does not meet the criteria.

B. Designation status

In July 2011, the designation system for specialized network security monitoring companies was implemented, and the government designated seven companies in October of the same year. After that, 15 companies were designated in 2018, 16 companies in 2019, and 17 companies in 2020. And, as 2 companies were newly designated in 2021, a total of 19 companies are operating as specialized network security monitoring companies as of December 2021.

The MSIT is constantly accepting applications for new designations and listening to relevant organizations to solve related difficulties in the industry.

Table 3-1-3-5 Current designation status of specialized network security monitoring company

	Company Name	Designated Date
1	CYBER ONE, Inc.	October 31, 2011
2	AHNLAB, Inc.	October 31, 2011
3	WINS Co., Ltd.	October 31, 2011
4	IGLOO SECURITY, Inc.	October 31, 2011
5	ADTCAaps, Inc.	October 31, 2011
6	KTIS, Inc.	October 31, 2011
7	KEPCO KDN Co., Ltd.	October 31, 2011
8	SECURE ONE, Inc.	April 27, 2012
9	KT, DS, Inc.	January 12, 2016
10	Samsung SDS, Inc.	August 5, 2016
11	PIOLINK, Inc.	October 18, 2017
12	Gabia, Inc.	October 18, 2017
13	A3SECURITY, Inc.	April 25, 2018
14	LOTTE DATA COMMUNICATION COMPANY	July 13, 2018
15	LG CNS, Inc.	July 13, 2018
16	SECUI Corporation	March 19, 2019
17	CMT Information & Communication Co., Ltd.	November 10, 2020
18	PDIC, Inc.	June 14, 2021
19	Shinhan DS, Inc.	October 18, 2021

3. Survey on Information Security Purchase Demand Data

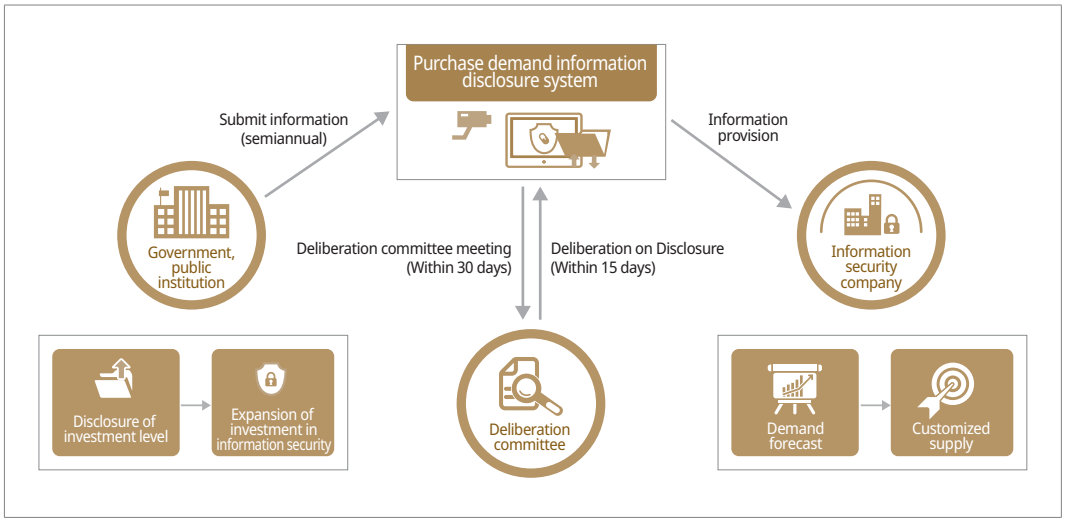
A. Overview

By Article 6 (Provision of purchase demand information) of the 「Act on the Promotion of Information Protection Industry」, the government surveyed twice a year for customized information technology development for providers. It forecasted the market for cybersecurity products and services in the public sector. This survey includes fixed purchase demand for the first half of the current year and expected purchase demand for the second half of the following year.

The government collects data from the public sector on demand for cybersecurity products- hardware and software - and services. Article 4 of the 「Enforcement Decree

of the Information Protection Industry Promotion Act」 requires the data related to the cybersecurity purchase demand. The government then reviews the data collected through the Purchasing Demand Information Deliberation Committee to determine whether it has a significant impact on national security and public interest and then posts it on the Information Security Industry Promotion Portal (www.ksecurity.or.kr) to provide it to companies.

Figure 3-1-3-1 The provision procedure of purchasing demand information

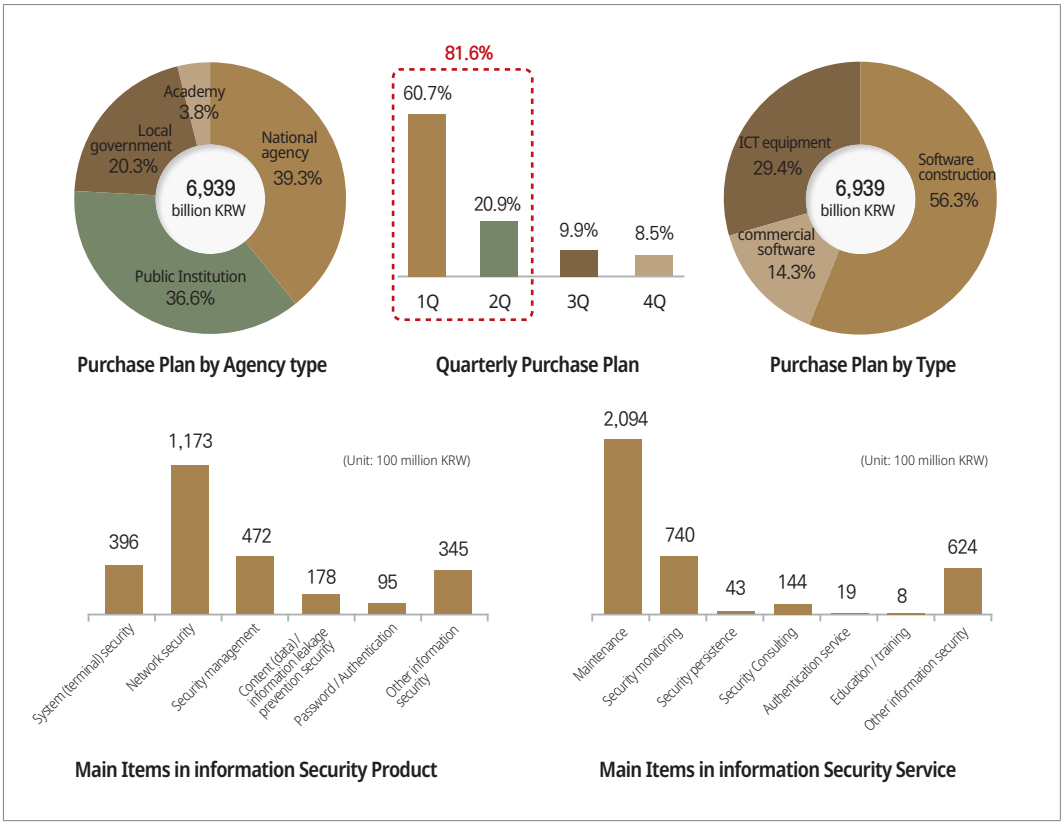


B. Cybersecurity purchasing demand survey data in 2021

From January to February 2021, the government surveyed 2,580 organizations – governmental institutions, public organizations, local governments, and educational organizations – on cybersecurity purchase demand data.

The total demand for cybersecurity purchases in 2021 was 693.9 billion KRW. State organizations accounted for 39.3% of the total with 273.1 billion KRW, public organizations for 36.6% with 253.9 billion KRW, and local governments for 20.3% with 140.7 billion KRW. The cybersecurity purchase budget accounted for 421.1 billion KRW (75.2%) in the first quarter and 145 billion KRW (20.9%) in the second quarter. Thus, the total cybersecurity budget skewed to 81.6% in the first half of the year.

Figure 3-1-3-2 Major result of fixed information security purchasing demand data in 2021



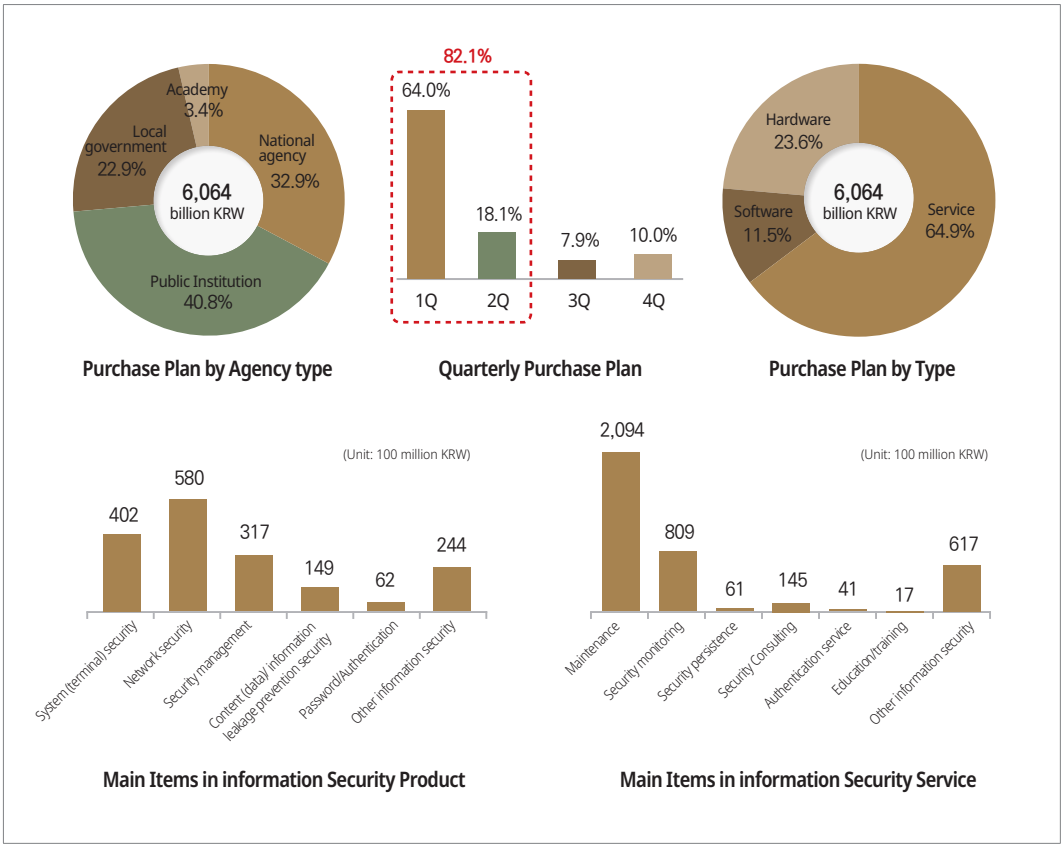
[Source: KISA]

By type, the budget for purchasing services was 390.8 billion KRW (56.3%), 204.1 billion KRW (29.4%) for hardware, and 99 billion KRW (14.3%) for software. System (terminal) security (39.6 billion KRW), security management (47.2 billion KRW), and network security (117.3 billion KRW) were the main items purchased. The items purchased for information security services are maintenance (209.4 billion KRW), network security monitoring (74 billion KRW), and security consulting (14.4 billion KRW).

C. Expected cybersecurity purchasing demand survey for 2022

From September to October 2021, the government surveyed 2,583 organizations – governmental institutions, public organizations, local governments, and educational organizations – on cybersecurity purchase demand.

Figure 3-1-3-3 Major results of expected cybersecurity purchasing demand data for 2021



[Source: KISA]

The total purchase amount of information security in 2021 is expected to be 606.4 billion KRW. Looking at the type of organization, the budget of public organizations was the highest at 247.4 billion KRW (40.8%). State organizations accounted for 32.9% of the total 247.4 billion KRW, and local governments accounted for 22.9% with 138.9 billion KRW. By order period, the cybersecurity budget for the first quarter was 388 billion KRW (64%), and 109.8 billion KRW (18.1%) for the second quarter. Thus, the total cybersecurity purchase budget skews in the first half of the year(82.1%).

By type, the budget for purchasing services was 393.4 billion KRW (64.9%), followed by hardware (143.2 billion KRW (23.6%)), and software (69.8 billion KRW (11.5%)). The main items in information security products are network security (58 billion KRW), system security (40.2 billion KRW), and security management (31.7 billion KRW). In addition, information security services mainly are maintenance (209.4 billion KRW),

network security monitoring (80.9 billion KRW), and other information security (61.7 billion KRW).

4. Information Security Data Disclosure

A. Overview

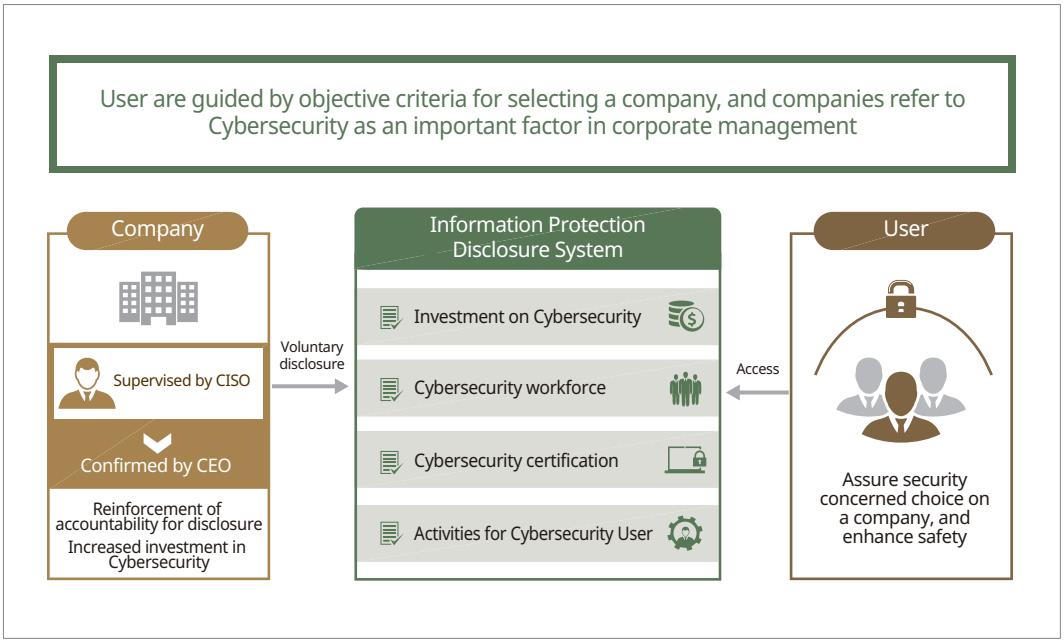
As the digital transformation accelerates, the ripple effect in the event of a cyber-infringement incident leads to economic loss at the national level beyond a specific company or individual level. As a result, the importance of information security is being emphasized.

To respond effectively to increasing cyber threats, companies must increase their investment in cybersecurity and disclose relevant information to minimize information asymmetry between companies and stakeholders, users, and people.

Nevertheless, administrators treated cybersecurity as a cost, and only certain groups that manage and supervise enterprises maintained cybersecurity status information. As a result, stakeholders make decisions without sufficient information.

Accordingly, an information security public announcement system was implemented that required companies to disclose certificates related to cybersecurity investment, personnel status, and information security. This system provides objective criteria for company selection for users and objectively identifies the level of information security for companies so that information security can be referred to as an essential factor when making business decisions.

Figure 3-1-3-4 **Information security disclosure system**



[Source: Guidelines for Disclosure of Information Security]

B. Basis of the Disclosure

The government developed the disclosure system by Article 13 of the 「Act on the Promotion of Information Security Industry」. As a result, information providers and intermediaries over information and communication networks can disclose 'cybersecurity statuses, such as investment, human resources, and certifications'.

To facilitate the smooth implementation of this disclosure, the MSIT distributed 「Guideline on Disclosure of Information Security 」, containing detailed information such as standards and methods for preparing the disclosure of information security, and enacted the 「Notification on Disclosure of Information Security 」. Nevertheless, the participation rate was low even five years after the introduction of the system, with only 52 companies disclosing the status of information security.

Accordingly, in 2021, the 「Act on the Promotion of Information Security Industry」 was amended to make information security disclosure mandatory for companies of a certain size or larger to promote safe internet use by information and communication service users and investment in information security by companies. It is expected that the information security level will be strengthened and the effectiveness of

the disclosure system will be improved as the mandatory disclosure of information security will induce companies to invest in information security.

C. Major contents of the disclosure system

Anyone who provides information or mediates the provision of information through the information and communications network may voluntarily disclose the cybersecurity status. However, a person who meets the criteria of Article 8 of the Enforcement Decree of the Act on the Promotion of Information Security Industry」 in consideration of business field, sales, and the number of users must disclose the current status of cybersecurity.

In the case of disclosing cybersecurity status, it is necessary to include the status of cybersecurity investment compared to information technology investment, cybersecurity personnel compared to information technology experts, certification/evaluation/inspection related to cybersecurity, and other cybersecurity activities for users of the information and communications services.

Furthermore, the disclosure body's CISO shall supervise the disclosure of cybersecurity status. The CEO shall review the contents of the disclosure and submit it to the disclosure authority by June 30 of each year. The disclosure authority shall publish the contents in the electronic disclosure system.

Those who are not subject to mandatory disclosure but have voluntarily followed information security disclosure can receive a 30% discount on the application fee (including initial, post, and renewal) when applying for Information Security Management System (ISMS) certification and Personal information & Information Security Management System (ISMS-P) certification.

D. Disclosure status of information security

In 2016, two companies joined the information security disclosure system, 10 companies in 2017, 20 companies in 2018, 30 companies in 2019, 45 companies in 2020, and 64 companies in 2021.

In 2021, the 6th year of system operation, companies and organizations of various industries and sizes, such as telecommunications, finance and shopping, participated

in the information security disclosure system. As of December 2021, 29 companies, including SK Telecom and Viva Republica, have disclosed their information security status for more than two consecutive years, and 35 companies, including CJ Korea Express, Daesang, and E-Mart, have newly implemented information security disclosure.

For information security status, please refer to the e-disclosure system of the Information Security Industry Promotion Portal (www.ksecurity.or.kr).

Chapter 2

Cybersecurity Technologies

Section 1 Overview

As the digital transformation has accelerated across the country and society due to the prolonged COVID-19, non-face-to-face societies such as telecommuting, video conferencing, and unmanned work have become common. Accordingly, security in digital and non-face-to-face environments is emerging as a critical issue. Based on the ultra-low latency of 5G, we have entered a hyper-connected society without on-offline boundaries, and the development of AI technology is accelerating the change into a super-intelligent society.

To move forward to the smart evolution towards secure, hyper-connected, super-intelligent society, core security technologies became even more important, therefore, it is necessary to strengthen security technology layers such as zero-trust, multi-cloud, and contactless authentication technology, for people can safely use non-face-to-face services.

Also, as the entire industry is going digital, ICT convergence will be the core infrastructure, and better security in services is required, plus, 5G mobile communication is rapidly deployed and the accumulated number of subscribers is

more than 10 million. Dramatic increase of convergence services using 5G services are deploying into our real lives such as autonomous vehicles and smart city, however, security problems remain that keeps people in anxiety.

To respond to 5G security problems already applied to many areas, there are many research activities on security measures such as national and public infrastructure, 5G edge computing, and autonomous cyber restoration technology. And beyond 5G, research on the next-generation communication (6G) must also be carried out in a timely manner.

As market competition in the field of new security technologies in major countries intensifies, it is necessary to secure core technologies to strengthen global competitiveness. To this end, it is necessary to continuously strengthen the researches that expand AI security technology to various security industry fields, which has been limitedly used in some fields such as cyber threat detection and antivirus. Moreover, in the process of introducing AI security technology to the industries, it should be based on balanced technology development that can respond to adverse effects such as the emergence of AI machine hackers.

Furthermore, to secure leadership in cybersecurity for next-generation infrastructure (6G, quantum computing, etc.), a strategic foundation for new security technology and the advanced cybersecurity technology development is underway one after another. Shaping the security posture on strategic future technologies is essential, such as, hyper-reliable core technology for secure 6G next-generation convergence service with no security concern, and early transition to secure quantum-resistant cryptographic infrastructure to counter the threat that quantum computers may decrypt cryptographic infrastructures such as RSA.

Along with the innovative development of digital technology, data are becoming an important production factor in economic activities such as the creation of new products and services. However, privacy issues arise such as re-identification and misuse of personal information caused by digitalized economy. There are ongoing researches in response to these problems, such as complex technology for de-identification of personal information, and homomorphic encryption technology that can utilize encrypted data without infringing on personal information.

Lastly, we must utilize security technology to counter cybercrimes that are advanced day by day and cause enormous damage to the public. We must make various efforts to solve the current social problems by source tracing technology, and securing investigation data related to cybercrimes of investment fraud, and drug dealing with ransomware and virtual currency.

We will look into the following issues: security in a non-face-to-face environment due to the spread of COVID-19, cloud and convergence security by digital transformation, full-cycle data security technology to revitalize the data economy after the 3 Data Acts, creation of a safe environment for a hyper-connected/intelligent society, and development of core technologies such as security technology to solve social problems.

Section 2 Core Technologies

1. Security technologies in COVID-19 era

A. Zero-trust security technology to provide secure non-face-to-face services

The prolonged COVID-19 pandemic has paralyzed social functions in many countries, causing social and economic loss. Therefore, each country is making efforts for a rapid recovery. In this situation, to rapidly encourage industrial activities, the government should provide secure ICT-based non-face-to-face services. More specifically, the government must solve the ever-increasing security threats of non-face-to-face services such as video-conferencing, telecommuting, online education and transactions and provide an environment where the general public can use secure non-face-to-face services.

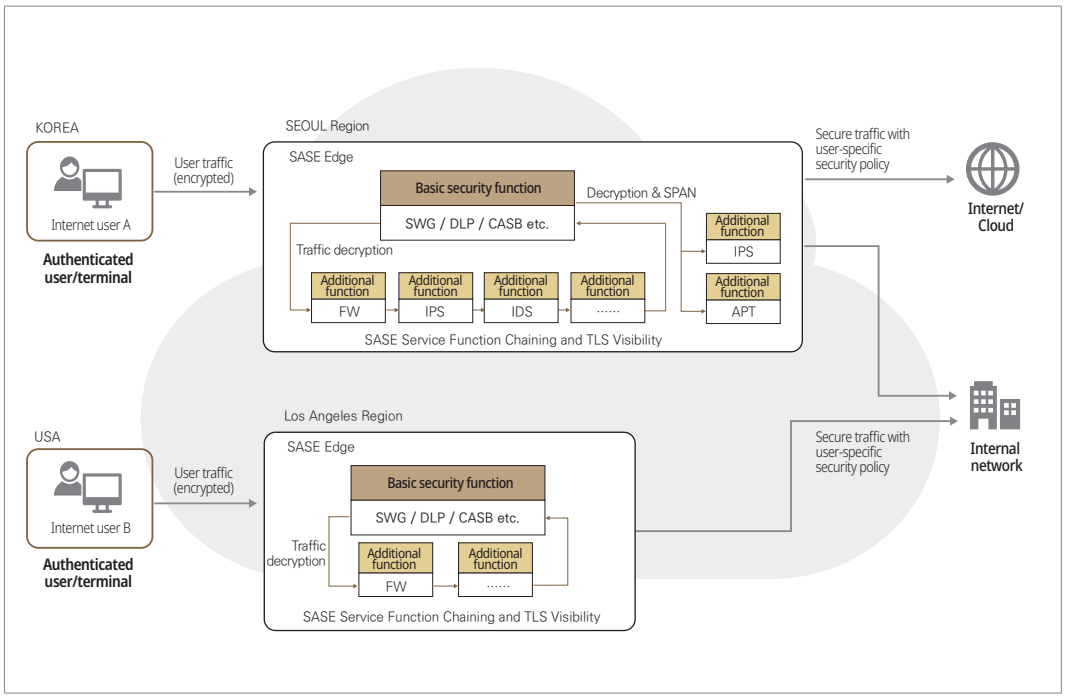
To cope with the increasing need for non-face-to-face services and provide secure non-face-to-face services by guaranteeing their reliability, the government is promoting zero-trust security technology.

B. Multi-cloud security technology to protect data and users when using non-face-to-face cloud services

As telecommuting and video-conferencing increase, the use of non-face-to-face cloud services is increasing. Along with the increase in usage, security threats to non-face-to-face cloud services are expected to increase. Accordingly, the need to develop security technologies to strengthen cloud infrastructure security is also increasing.

In order to cope with this situation, the government is promoting technology development that can predict and respond to security threats that may occur in cloud computing executable environments (containers, serverless, etc.), and the development of Secure Access Service Edge (SASE), which includes network and communication integration due to cloud infrastructures and services integration.

Figure 3-2-2-1 Conceptual diagram of SASE-based integrated intelligent edge technology



C. Unmanned security and contactless authentication technology for unmanned service environment safety

With the spread of non-face-to-face services, the number of unmanned stores such

as convenience stores and cafes is increasing in Korea. As the number of unmanned stores increases, so does the need for physical and IT security of unmanned stores. In addition, the need for contactless authentication technology for non-face-to-face services (bank, payment, etc.) is also increasing.

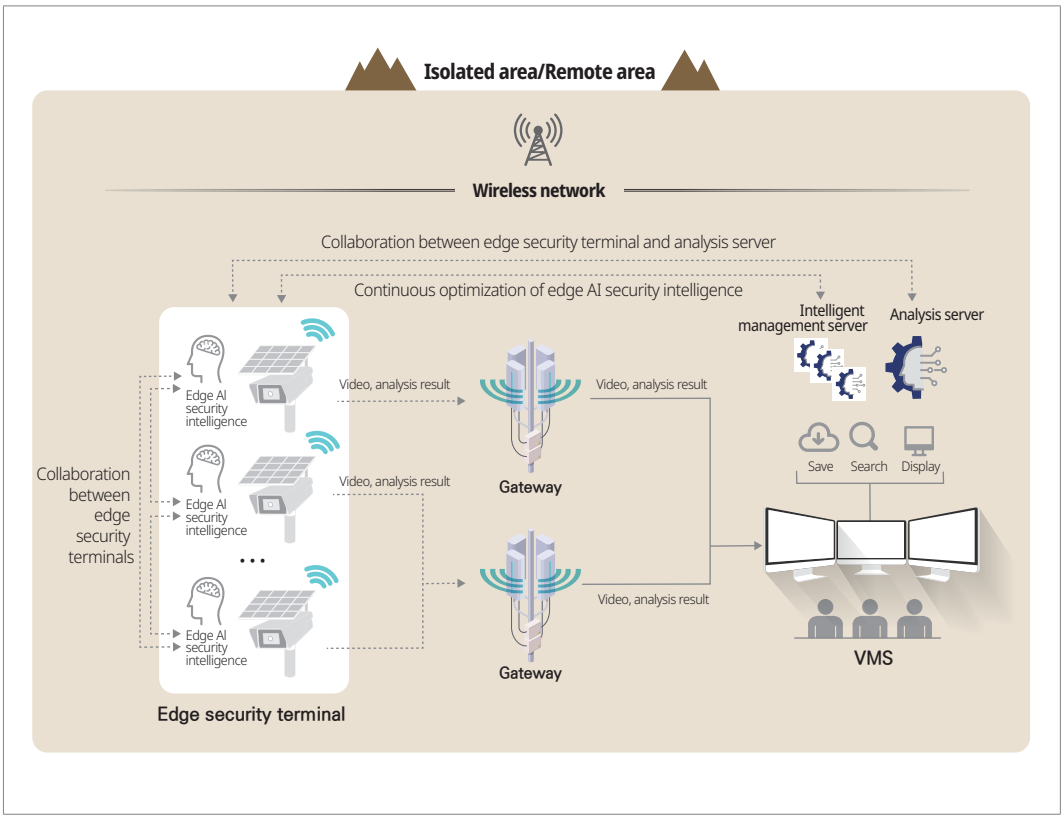
2. Technologies to strengthen the security of ICT convergence core infrastructures and convergence services due to industrial digitalization

A. Security technology development for 5G MEC infrastructure

Mobile edge computing is the 5G high-speed data processing technology that supports real-time/high-quality services by placing users and servers in near locations, and 5G MEC (Mobile Edge Computing) infrastructure will be expanded for ultra-low latency/high-quality application services. Likewise, mobile edge computing security is emerging as a hot topic.

Regarding the development of mobile edge computing security technology, the government plans to promote the development of a wireless edge video surveillance system that supports continuous optimization of edge AI security functions, and collaboration with edge security terminals.

Figure 3-2-2-2 Conceptual diagram of wireless edge video surveillance system



B. Security technology to secure 5G convergence services such as 5G-based national/public infrastructures, autonomous vehicles, and smart city

Currently, 5G communication technology is being used in convergence with diverse sectors of autonomous vehicles, smart city, and national/public infrastructure services including control, administration, and medical care. In preparation for the further spread of various 5G convergence services, there is a need for security technology for 5G convergence services.

In 5G convergence services, the government plans to apply security technologies with pilot/empirical applications to critical information and communications infrastructures resulted from the national research and development projects, and after the performance assessments, will deploy phase-by-phase. Moreover, the government plans to develop security technologies for emerging 5G convergence services.

C. Autonomous response enabled cyber restoration technology to prevent cyberattacks on 5G infrastructures

5G infrastructures expand and have more cross-sections with many areas, so does the cyber threats. Technology demand arises that can mitigate the damage caused by cyberattacks, and quickly restore the system to the state before the incidents or troubles.

For this reason, the government is promoting the development of cyber resilience technology to autonomously respond to increasing cyber threats (malicious traffic, unauthorized access, etc.).

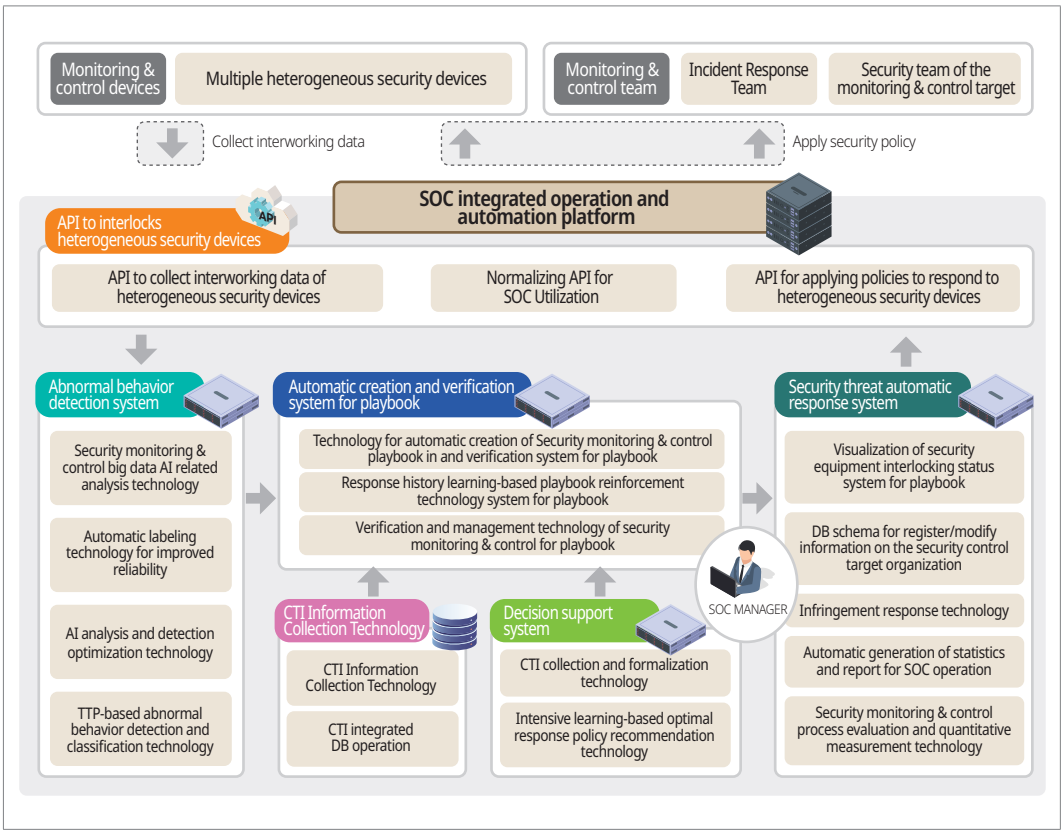
3. Securing Global Leading Cybersecurity Technologies

A. Artificial Intelligence-based Security Technology

While researches on AI-based security technology is active at home and abroad, it is important to develop a balanced security core technology to counteract the negative functions of AI (emergence of AI machine hackers, increasing threats on AI) along with strengthening the good function of AI (application of AI security technology). To overcome the limit of human analysis due to the increasing sophistication/secrecy of AI hackers and large-scale tera-level attacks, a technology is demanded that can automatically analyze security threats in new ICT environments based on AI and big data technology, and can analyze and respond to the smarter cyberattacks.

Cybersecurity orchestration and automatic response technology based on AI and big data automatically classify and detect large-scale security threats that occur in various ICT environments such as heterogeneous security solutions and domains through building high-quality data. It also leads to the development of technology that automates the entire process of the incident response process (monitoring-analysis-response) when dealing with intelligent cyber threats.

Figure 3-2-2-3 Conceptual diagram of intelligent cyber security control technology



Furthermore, a new technology is demanding to raise competitiveness of AI security technology, such as the core source technology of cyber offense and defense based on self-evolving AI and analysis techniques for digital evidence using AI technology. In addition, it is necessary to strengthen the global competitiveness of the domestic security industry by establishing an ecosystem that can be applied to various industries required in the field.

B. Future Strategic Security Technologies

As competition for technological hegemony is intensifying among leading countries, securing security technology is strategically important to take the lead in cybersecurity in the future infrastructure environment. At the same time, as the era of ultra-low latency and hyper-connectivity opens, it is necessary to prepare for security threats to future infrastructure.

Accordingly, the government is making an effort to develop 6G security source technology to provide a secure infrastructure free from cyber threats caused by changes in the 6G future environment. At the same time, the government has secured a 6G security standard patent to develop a security embedded architecture technology that guarantees essential security quality from the 6G design stage and to preoccupy the global market. Furthermore, it is promoting the development of 3D space mobile satellite communication security technology to ensure hyperspace availability.

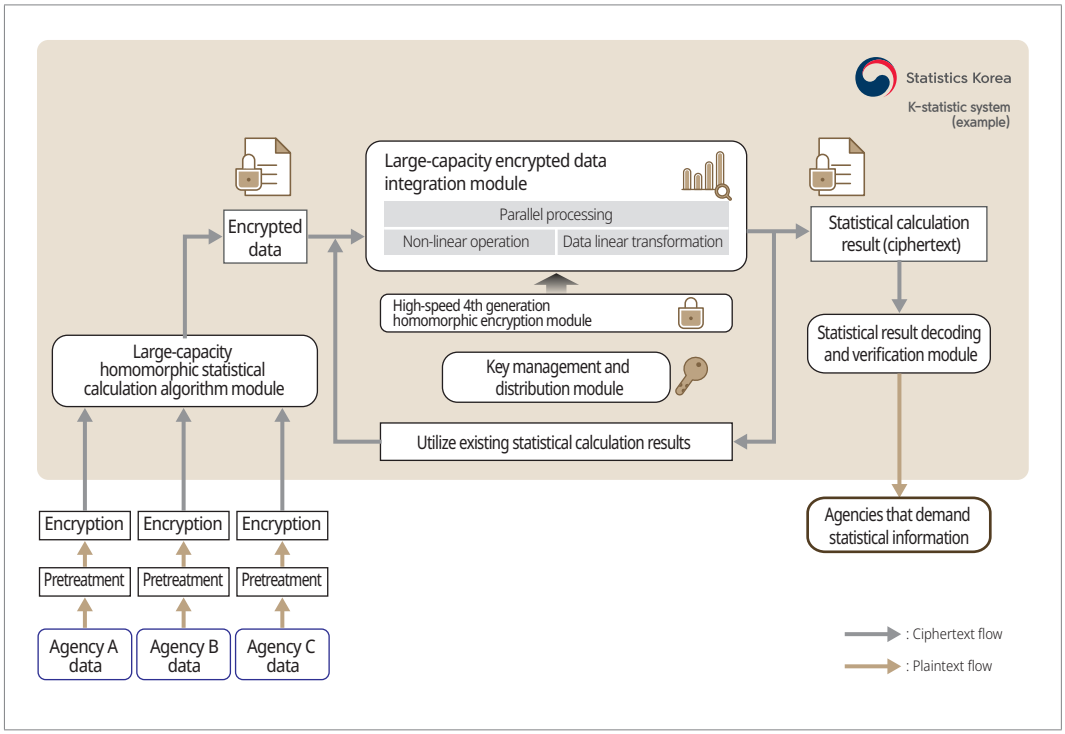
With regard to quantum cryptography technology, the government is aiming for early transition and support to a secure quantum-resistant cryptography infrastructure to counter the threat of decryption of cryptographic infrastructure by quantum computers. The government has developed important technologies including quantum-resistant PKI considering the application of security services such as 5G/6G security and smart city. Also, it is developing implementation technologies that take into account various environmental and security threats. In addition, the government is promoting the development of cryptographic module safety standards and test/evaluation technology for the safe use of quantum-resistant cryptography in connection with smart cities.

4. Data Security Technologies for Digital Economy

A. Data De-identification for Privacy

A digital economy refers to an economic structure in which data is used as an important production factor in economic activities such as the creation of new products and services along with the innovative development of digital technology. Even now, de-identification such as pseudonymous/anonymous processing of data is being performed to strengthen privacy centered on specific application environments (medical, image, etc.). However, due to the expanding digital economy, the demand for data de-identification technology is increasing in all areas.

Figure 3-2-2-4 **Conceptual diagram of statistical analysis algorithm and module using homomorphic encryption**

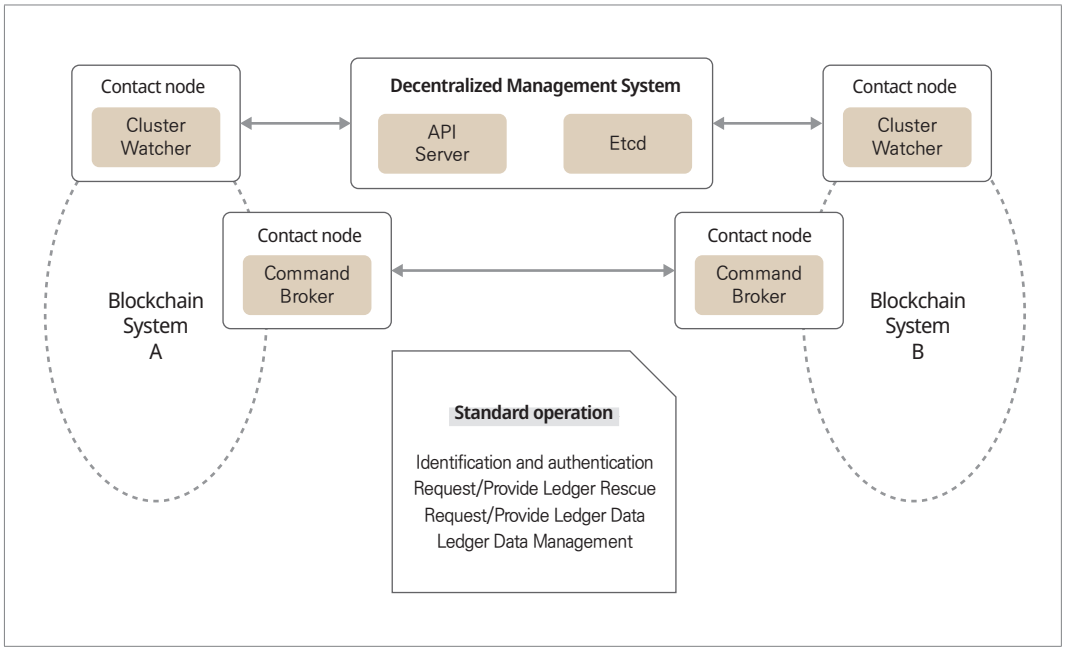


Statistics Korea, K-statistic system (example)

To respond to this, the government is promoting the development of the following technologies: multiplexing techniques for de-identification processing (pseudonym processing, data deletion, categorization, masking, etc.) according to data characteristics and the scope of use by the different environments, differential privacy technology that protects privacy while maintaining statistical characteristics, and technology of homomorphic encryption that can be operated while data is encrypted. Moreover, the government is trying to facilitate the development of technologies for data classification and evaluation and tracking of misuse and abuse data to prevent risks arising from data combination and illegal recombination.

B. Development of encryption and utilization technology for distribution-oriented data security

Figure 3-2-2-5 **Concept diagram of service data convergence and interoperation technology between heterogeneous blockchain systems**



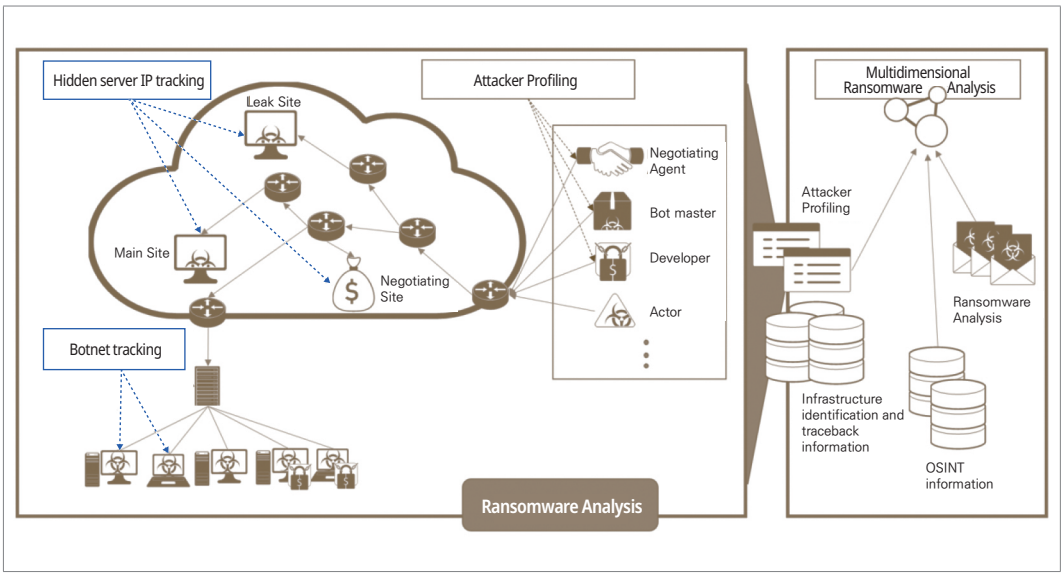
[Source: Institute of Information & Communications Technology Planning & Evaluation]

To revitalize the digital economy, not only technology to protect stored data, but also security and technical standards for the data distribution process used as important resources are required. Therefore, for data exchange and recombination between heterogeneous systems, the government is promoting the development of technologies such as homomorphic and functional cryptography that can process information in an encrypted state, rather than using an external system or going through a centralized trusted institution. The government is also developing technologies that can minimize damage caused by reliability problems or service failures by decentralizing the structure of the data processing system.

5. Security Technologies for Digital Crime Prevention and Daily Life

A. Tracking Technology and Better Capabilities for Cybercrimes

Figure 3-2-2-6 Conceptual diagram of ransomware attack source identification and analysis technology



[Source: Institute of Information & Communications Technology Planning & Evaluation]

Damage by the cybercrimes is getting increasingly worse, which are becoming more intelligent and penetrating deeply into people's lives. Accordingly, to secure evidence and trace the source of cybercrime, it is getting more important to have faster responses, as well as identifying and detecting cybercrime infrastructures, profiling, and attack tracking technology.

Thus, the government is facilitating the development of the following technologies to collect, identify, and track information on cybercriminal behavior and attack groups: Dark web hidden service identification and source tracking technology and lifecycle-based attack group identification and type analysis technology.

Besides, to respond to evolving ransomware such as RaaS (Ransomware as a Service), the relevant attack infrastructure must be identified by static and dynamic analysis technology specialized for ransomware. At the same time, similarity analysis

and grouping between ransomware are also required. Therefore, the government is developing a technology to identify and analyze the source of a ransomware attack that can quickly respond to the attack by determining the possibility of data recovery based on the analyzed ransomware vulnerability, etc., and recognizing the characteristics of the attacking organization.

6. Lead Cybersecurity Standards, Enhance Industry Competitiveness

A. National Cybersecurity Standards

To strengthen cybersecurity for digital transformation and foster the industry, the government is preemptively developing national standards for many areas of cybersecurity. The national cybersecurity standards are based on international standardization activities participated by local experts from industry, academia, and research in a wide range of areas including cybersecurity management, personal information protection, encryption algorithm, and cybersecurity threat response, and being developed in correspondent with the Korean language so that can be used widely by industry.

In 2021, a total of 11 national standards in cybersecurity were enacted and revised in the fields of personal information protection, cybersecurity management, encryption algorithm, security product evaluation, and biometric security.

Regarding the detailed national cybersecurity standardization status of publishing and revision, the following matters were announced in 2021: personal information impact assessment guideline (KS X ISO/IEC 29134) that can be used to review and mitigate security threats that may arise in the process of processing personal information as part of revitalizing the digital economy, competency requirements for cybersecurity management experts (KS X ISO/IEC 27021), which is a standard for the competence of experts involved in establishing, implementing, maintaining, and improving cybersecurity management in organizations, n-bit block cipher operation mode (KS X ISO/IEC 10116) for confidentiality protection during data transmission and storage.

Table 3-2-2-1 National Cybersecurity Standardization Status

	Standard number	Standard name	Date of enactment and amendment
Revision	KS X ISO/IEC 10116	Information technology - security technology - n-bit block cipher operating mode	April 30, 2021
Revision	KS X ISO/IEC 10118-4	Information Technology - Security Technology - Hash Functions - Part 4: Hash Functions Using Legal Operations	
Revision	KS X ISO/IEC 14888-2	Information Technology - Security Technology - Additive Digital Signature - Part 2: Integer Factorization-Based Mechanism	
Revision	KS X ISO/IEC 14888-3	Information Technology - Security Technology - Additive Digital Signatures - Part 3: Discrete Algebra-Based Mechanisms	
Enactment	KS X ISO/IEC TR 15446	Information Technology - Security technology - Development guidelines for protection profile and security target	April 30, 2021
Enactment	KS X ISO/IEC 27021	Information Technology - Security technology - competency for information security management system experts	
Enactment	KS X ISO/IEC 29134	Information Technology - Security Technology - Personal Information Impact Assessment Guidelines	
Enactment	KS X ISO/IEC 17922	Information Technology - Security technology - Remote biometric authentication framework using biometric hardware security module	
Enactment	KS X ISO/ IEC19794-15	Information Technology - Biometric Data Exchange Format - Part 15: Palmistry Image Data	
Enactment	KS X ISO/IEC 30107-2	Information Technology - Biometric Presented Attack Detection - Part 2: Data Format	
Enactment	KS X ISO/IEC 30107-3	Information Technology - Biometric Presented Attack Detection - Part 3: Testing and Reporting	
Total	7 Enactment, 4 Amendment		

B. Cybersecurity Group Standards Development

The purpose of cybersecurity group standardization is to establish secure data ecosystems in line with government policy directions such as the Digital New Deal and K-Cyber Prevention and to build a secure digital nation. To this end, the government is promoting the standardization of next-generation security technologies applicable to many areas in consideration of quantum computing and hyper-connected network environments. The Information Security Technical

Committee (TC5) under the ICT Standardization Committee operated by the Telecommunications Technology Association (TTA) is developing group standards for domestic cybersecurity and focuses on developing standards for the cybersecurity infrastructures, personal information protection/ID management, blockchain security, cybersecurity, application security, evaluation and certification, and biometric technology.

In 2021, TC5 published and revised 23 group standards and 1 technical report, and in particular, developed the standards promptly on personal privacy protection and secure personal authentication to deal with the spread and continuation of COVID-19, and more specifically, provided control guidelines for mitigating Personally Identifiable Information (PII) protection threats that may occur in the process of managing infectious disease data by publishing the 'Privacy Protection Guidelines for Infectious Diseases Control and Prevention'. In addition, TC5 published the 'Digital Entry Logging Procedures Using Beacon-Based Dynamic Authentication Information', to provide a convenient and safe procedure for visiting records using beacon-based dynamic authentication information between users and facility terminals when creating a smartphone-based digital entry log for the prevention of infectious diseases. By safely managing and processing infectious disease-related personal information without information breach or exposure problems, these standards will ensure data security in the individual aspect and contribute to the increase of data use in the industrial aspect.

C. Cybersecurity Standards Activities

As cybersecurity threats become increasingly more intelligent and advanced, it is required to apply security technologies based on globally agreed cybersecurity standards and to make a joint response to global security threats. Accordingly, cybersecurity experts in the industry, academia, research, and related organizations are working to develop source technologies for effective response to cyber threats and strengthen the competitiveness of the cybersecurity industry and propose to the International Telecommunication Union (ITU), ISO/IEC JTC 1 (International Organization for Standardization / International Electrotechnical Commission Joint Technical Committee, ISO/IEC Joint Technical Committee).

ITU-T SG17 (Study Group 17 Security) is responsible for developing international

standards on security application service technologies from the viewpoint of information communication. Specifically, SG17 is developing international standards related to network security including 5G, information security management system, cybersecurity and spam response, application service security, identity management and telebio recognition technology, vehicle communication security, distributed ledger security, quantum-based security, and general technologies that support security applications such as public key infrastructure. Professor Heung-Yeol YOUM in Soonchunhyang University took over the SG17 chairman, and domestic chairmen, vice-chairmen, and editors are actively developing standards.

ISO/IEC JTC 1/SC 27 (Sub Committee 27, Information Security, Cybersecurity, Privacy Protection) is responsible for developing international standards on general methods and technologies for information technology security under ISO/IEC JTC 1. Specifically, SC 27 is developing international standards on information security management systems, encryption algorithms and security mechanisms, security evaluation standards, security control and service, personal information protection, and identity management. Moreover, SC 27 is actively reflecting the encryption algorithm and personal information protection technology developed as domestic technology to international standards.

The government and the industry, academia, and research will continue to carry out these vigorous international standardization activities in the future to secure leadership in global cybersecurity standards and strengthen the competitiveness of the security industry.

Section 3 Conventional Technologies

The Korea Information Security Industry Association surveyed the 1,283 domestic cybersecurity companies (531 information security and 752 physical security), and the results of the '2021 Survey of Information Security Industry' were used.

1. Operation of Center and responsible department in information security companies

The survey identified that 208 companies(39.2%) operate a company-affiliated research center, and 256 companies(48.2%) use a responsible department for R&D. Moreover, 67 companies (12.6%) did not operate both a company-affiliated research center and an R&D department. It appears that more than 80% of information security companies are working on their technology development and research.

Among the 308 companies operating an affiliated research center, 92 companies had between 20 and 100 employees, and 88 companies had fewer than 20 employees.

Table 3-2-3-1 Operational status of dedicated technology research centers and departments for information security companies

(Unit of measurement: units, %)

	Number of Staff				Total	Ratio
	Fewer than 20 people	Between 20 and 100 people	Between 100 and 200 people	200 or more		
Operation of company-affiliated research center	88	92	10	18	208	39.2%
Operation of R&D department	84	129	29	14	256	48.2%
None	47	16	4	0	67	12.6%
Total	219	237	43	32	531	100.0%

2. Investment in technology development

According to the survey, in 2021, 237 companies that have investment assets would spend 1,227.4 million KRW on average, and 236 companies would spend 968.5 million KRW on R&D.

The average investment in technology R&D has increased continuously, and it is 7.16% in 2020 and 7.30% in 2021 when converted into a sales percentage.

Table 3-2-3-2 Information security company's annual technology development investment

(Unit of measurement: units, million KRW, %)

	2020		2021	
	No. of companies	Average investment	No. of companies	Average investment
Total investment(R&D / building /machinery and equipment, etc.)	237	1,127.1	237	1,227.4
R&D investment	236	876.9	236	968.5
Ratio of investment to sales (%)	7.16		7.30	

3. Intellectual property rights

As a result of a survey on the information security-related intellectual property right, the intellectual property rights acquired or ready for registration are 3,169 cases. In detail, 2,909 acquired intellectual property rights and 260 intellectual property rights are pending.

The acquired information security intellectual property rights comprises 1,977 patent rights (68.0%), 268 utility model rights (9.2%), 111 design rights (3.8%), and 553 trademark rights (19.0%).

Information security intellectual property rights pending were surveyed as 227 patent rights (87.3%), 6 utility model rights (2.3%), and 27 trademark rights (10.4%).

Table 3-2-3-3 Information security-related intellectual property rights

(Unit of measurement: units, %)

		Acquired		Application	
		Cases	Rate (%)	Cases	Rate (%)
Intellectual property right	Patent right	1,977	68.0	227	87.3
	Utility model right	268	9.2	6	2.3
	Design right	111	3.8	0	0.0
	Trademark right	553	19.0	27	10.4
Total		2,909	100.0	260	100.0

Meanwhile, 81 companies owned foreign patents, 221 cases, with an average of 2.7 per company. Twenty companies are currently processing the patents, having 41 processing applications, holding an average of 2.1 applications per company.

Table 3-2-3-4 Information security foreign patents

(Unit of measurement : units, %, cases)

	No. of companies	Percentage of companies(%)	Total number	Average number
Acquired	81	15.3	221	2.7
Application	20	3.8	41	2.1

4. Export

The exports of the information security industry were 122,766 million KRW in 2019, and 2020's exports have been growing by 19.5%, its amount is 145,592 million KRW. Looking at the proportion of exports in 2020, exports of information security system development and supply accounted for 64.4% of total exports, higher than information security-related services(35.6%).

Table 3-2-3-5 Cybersecurity export status by major categorys

(Unit of measurement: million KRW, %)

	2019	2020	Growth rate(%)	Importance(%)
Development and supply of information security system	78,039	93,846	20.2	64.4
Information security related services	44,728	51,746	15.6	35.6
Total	122,766	145,592	19.5	100.0

In the information security system development and supply sector, network system product exports account for the most significant portion of the export market, 52,799 million KRW in 2020. The second-largest product is the system security solution at 13,005 million KRW. The product with a significant increase in exports is developed for network security systems, showing a relatively considerable growth rate(45.5%).

Among information security-related services, the exports in 2020 were 23,139 million KRW for security consulting services, an increase of 1.5%.

Table 3-2-3-6 Exports of information security products and services

(Unit of measurement: million KRW, %)

		2019	2020	Growth rate(%)
Information security system development and provision	Network security system development	36,267	52,799	45.5
	System security solution development	12,853	13,005	1.1
	Information leakage prevention system development	12,726	12,277	-3.6
	Password/authentication system development	5,551	6,063	9.2
	Security management system development	10,641	9,702	-8.8
Information security related services	Security consulting services	23,104	23,139	1.5
	Security system maintenance/security continuity services	8,049	13,009	61.6
	Security control services	8,103	9,656	19.1
	Security education and training services	-	-	-
	Public/private certificate	-	-	-
	Cloud services	5,471	5,945	8.6
Total		122,766	145,592	18.5

Chapter 3

Cybersecurity Workforce

Section 1 Overview

According to the '2021 Survey of Information Security Industry', as a result of a survey of 1,283 domestic information security companies (531 information security, 752 physical security), the number of cybersecurity industry personnel is 54,706 as of December 2020. Among them, the number of information security personnel is 15,832 (28.9%), and the number of physical security personnel is 38,874 (71.1%).

By position, there were 4,774 (8.7%) technicians with over 15 years of experience, 6,695 (12.2%) technicians with between 11 and 15 years of experience, 11,171 (20.4%) technicians with between 7 and 11 years of experience, 15,488 (28.3%) technicians with between 4 and 7 years of experience, and 16,578 (30.3%) technicians with under 4 years of experience.

Table 3-3-1-1 Security industry workforce

(Unit of measurement: persons, %)

	Information security	Physical security	Total					
			<4 years	4~<7 years	7~<10 years	11~<15 years	15+ years	Total
No. of persons	15,832	38,874	16,578	15,488	11,171	6,695	4,774	54,706
Rate	28.9	71.1	30.3	28.3	20.4	12.2	8.7	100.0

According to the status of manpower by sales size in the cybersecurity industry, it was found that companies with sales of 10 billion or more have 42,983 employees out of 54,101 total employees, companies with sales of less than 1 billion have 1,828 employees, companies with sales of more than 1 billion and less than 5 billion have 5,931 employees, and companies with sales of more than 5 billion and less than 10 billion have 3,359 employees.

Table 3-3-1-2 Manpower by sales volume in security industry (as of December 2020)

(Unit of measurement: persons)

	<4 years	4~<7 years	7~<10 years	11~<15 years	15+ years	Total
<1 billion KRW	503	636	417	161	111	1,828
1~<5 billion KRW	1,872	1,868	1,297	620	274	5,931
5~<10 billion KRW	1,048	972	690	369	280	3,359
10+ billion KRW	12,978	11,925	8,620	5,558	3,902	42,983
Total	16,401	15,401	11,024	6,708	4,567	54,101

In 2020, a total of 4,618 people were recruited by cybersecurity companies, including 2,601 (56.4%) new employees and 2,017 (43.6%) experienced employees.

Table 3-3-1-3 Employment in cybersecurity industry (as of December 2020)

(Unit of measurement: persons, %)

	Information security			Physical security			Total		
	New	Experienced	Subtotal	New	Experienced	Subtotal	New	Experienced	Total
No. of persons	1,061	711	1,772	1,540	1,306	2,846	2,601	2,017	4,618
Rate	59.1	40.1	100.0	54.2	45.8	100.0	56.4	43.6	100.0

In 2021, the total number of persons for new recruitment plans by cybersecurity

companies is 4,009, including 2,213 (55.2%) new employees and 1,796 (44.8%) experienced employees.

Section 2 Cybersecurity Curriculum

According to a survey of cybersecurity departments in universities and graduate schools in 2021, a total of 126 departments are operated, including 17 in junior colleges, 50 in universities, and 59 in graduate schools. In 2021, the number of enrolled students in regular education institutions of junior colleges or higher was 9,158.

1. Junior college

Departments related to cybersecurity at junior colleges mainly teach computer (cyber) information security, and as of 2021, the number of enrolled students was 1,055.

Table 3-3-2-1 Departments related to information security at junior colleges in 2021

(Unit of measurement: persons)

University	Department	Number of enrolled students
Gimpo University	Department of Cyber Security Technology (3-year course)	62
	Department of Cybersecurity Technology	10
Taegu Science University	Major in Information Security	Newly Established
Daejeon Institute of Science and Technology	Department of Computer Communication & Security	32
Dong Seoul University	ICT Security Major	131
	Department of ICT Security	15
	Major in Information Security	94
Doowon Technical University College	Department of Information and Communication Security Engineering	10
Myongji College	Internet Security Engineering as a Service	166
Baehwa Women's University	Department of Software & Security Convergence	86
Bucheon University	Department of Computer Information Security	113
Shingu College	Information & Communication Security	140

University	Department	Number of enrolled students
Yeungnam University College	Cybersecurity Division	53
	Department of Cybersecurity	21
Chosun College of Science and Technology	Department of Computer Security	57
Korea National University of Welfare	Department of Computer Information Security	47
Seoul Gangseo Campus of KOREA Polytechnics	Information Security Department (Convergence Security Software)	18
Total	17	1,055

[Source: Higher Education in KOREA, www.academyi21nfo.go.kr]

2. University

As universities and graduate schools establish new departments of cybersecurity or change existing departments to cybersecurity-related in order to systematically cultivate human resources through a regular curriculum, that the number of departments related to cybersecurity is increasing. In 2021, 6,639 students were enrolled in the cybersecurity department at universities.

Recently, as cybersecurity incidents have rapidly increased and threatened the lives, safety and property of the people, public interest in the importance of cybersecurity has also increased. Cybersecurity has become a national core issue. Reflecting these social interests and importance, the importance and necessity of personnel training for cybersecurity are also growing. In addition, as security threats spread through various ICT convergence products and services along with the recent changes in the ICT environment, departments related to convergence security are expected to emerge.

Table 3-3-2-2 Departments of cybersecurity related in universities in 2021

(Unit of measurement: persons)

University	Department	Number of enrolled students
Konyang University	Department of Cybersecurity Engineering	120
Kyungnam University	Department of Information Security	78
Kyung Hee Cyber University	Department of AI Cybersecurity	68
Korea University	Division of Smart Security	30
Korea University (Sejong)	Department of AI Cybersecurity	35
The Cyber University of Korea	Department of Information Management & Security	286
Gwangju University	Department of Cyber Security & Police	36
Kookmin University	Department of Information Security Cryptography Mathematics	188
Far East University	Department of Hacking & Security	98
Korea Nazarene University	Department of IT Broadcasting and Video Convergence (Information Communication Security)	52
Dankook University	Department of Industrial Security	48
Daegu Catholic University	Department of Cybersecurity	131
Daegu University	Computer & Information Engineering (Department of Information Security)	28
Daejeon University	Department of Information Security	168
Duksung Women's University	Major in Cybersecurity	29
Dongguk University	Department of Transdisciplinary Security	149
Tongmyong University	Department of Software Convergence Security	151
Dongseo University	Cyber Police Security major	Newly Established
	Department of Information Security	60
Dongshin University	Department of Convergence Information Security	144
Mokpo University	Department of Information security	133
	Department of Computer Information Security	15
Pai Chai University	Department of Cybersecurity	59
Busan University of Foreign Studies	Department of Information Security	89
Sangmyung University (2nd Campus)	Department of Information Security	158
Sangji University	Department of Information Security	28
Seoul Cyber University	Department of Big Data Information Security	426

University	Department	Number of enrolled students
Seoul Women's University	Department of Information Security	380
Seowon University	Department of Information Security	125
Sungshin Women's University	Department of Convergence Security Engineering	307
Sejong University	Department of Information Security	123
Sejong Cyber University	Department of Information Security	322
Suwon University	Department of Information Security	158
Soon Chun Hyang University	Department of Information Security	349
Ajou University	Department of Cybersecurity	193
Yeongsan University	Major in Cybersecurity	26
Woosuk University	Department of Information Security	145
Woosong University	Department of IT Convergence Smart IT Security Major	155
	Department of IT Computer Information Security Major	206
Uiduk University	Department of Police and Cybersecurity	87
U1 University	Department of Information and Communication Security	110
Ewha Woman's University	Major in Cybersecurity	153
Jeju International University	Department of Information Security Engineering	15
Chosun University	Department of Information and Communication Engineering (Embedded Security Major)	71
Joongbu University	Major in Information Security	194
Chung-Ang University	Department of Industrial Security	191
Cheongju University	Department of Digital Security	88
Hansei University	Department of Industrial Security	94
Hanyang Cyber University	Department of Hacking Security	315
Howon University	Department of IT Software Security	25
Total	50	6,639

[Source: Higher Education in KOREA, www.academyinfo.go.kr]

3. Graduate school

Recently, as the convergence between industry and ICT rises, new departments and majors related to convergence security are constantly being established. In 2021, there were 59 cybersecurity courses in graduate schools, with 1,464 students enrolled.

Table 3-3-2-3 **Cybersecurity related courses in graduate schools, 2021**

(Unit of measurement: persons)

University		Department	Number of enrolled students
General Graduate School of Gachon University		Department of Information Security	Newly Established
Kangwon National University	Graduate School	Department of Convergence Security	8
	Graduate School of Information Science & Public Administration	Department of IT Convergence	2
Konkuk University	Graduate School	Department of IT Convergence Information Security	3
	Graduate School of Information and Telecommunications	Department of Information Security	
Kyungpook National University Graduate School		Cooperative course between departments of information security science	64
Kyungil University Graduate School		Department of Cybersecurity	3
Korea University Graduate School	Graduate School	Department of Information Security	6
	Graduate School of Cybersecurity	Department of Information Security	55
		Department of Public Security Policy	1
		Department of Financial Security	18
		Department of Financial Security Major in Financial Security Policy	19
		Department of Big Data Application and Security	5
		Department of Cybersecurity	44
		Department of Convergence Security	14
		Department of Digital Forensics	193
	Graduate School of Computer & Information Technology	Department of Software Security	30
Korea University Graduate School (Sejong)		Department of Cybersecurity	2

University		Department	Number of enrolled students
Kookmin University	Graduate School	Department of Financial Information Security Cooperative Course	35
		Department of Security Smart Air Mobility	10
	Graduate School of Legal Affairs	Major in Security Law	10
Far East University	Graduate School of Industry Technology Security	Department of Technology Security	0
		Major in AI Security	3
	Graduate School	Major in AI Security	2
Specialized Graduate School of Namseoul University		Department of Big Data Industrial Security	5
Dankook University Graduate School of Public Administration and Legal Studies		Department of Convergence Security	43
Daejeon University	Graduate School of Business Administration, Public Administration & Social Welfare	Department of Cyber Forensics	Newly Established
	Graduate School	Department of Information Security	1
Dongguk University Graduate School of International Affairs and Information Security		Department of Cyber Forensics	52
		Department of Information Security	69
Myongji University	Graduate School	Security Management Engineering Interdisciplinary Course	42
	Graduate School of Industrial Technology	Department of Convergence Security	18
Mokpo National University	Graduate School	Information Security Technology Cooperative Course	2
	Graduate School of Industrial Technology	Major in Information Security	3
Pai Chai University Graduate School		Department of Cybersecurity	23
Pukyong National University Graduate School		Department of Information Security	6
Graduate School, Catholic University of Pusan		Engineering Master Course	3
Graduate School, Busan University of Foreign Studies		Department of Smart Convergence Security	7
Sogang University Graduate School of Information & Technology		Major in Information Security	33

University		Department	Number of enrolled students
Sungkyunkwan University Graduate School of Information and Communications		Department of Information Security	78
Sejong University Graduate School		Department of Information Security	39
Sejong Cyber University Graduate School of Information Security		Department of Information Security	139
Soon Chun Hyang University	Graduate School	Department of Smart Convergence Security	10
		Department of Information Security	14
	Graduate School of Future Convergence	Department of Information Security	2
Soongsil University Graduate School of Information Science		Department of Information Security	44
Graduate School of Ajou University		Department of Cyber Space	Newly Established
Inje University Graduate School		Department of Industrial Convergence Security	14
Inha University	Graduate School	Major in Industrial Security Governance	29
Chonnam National University Graduate School		Information Security Cooperation Course	59
Jeonbuk National University Graduate School		Department of Information Security Engineering	3
Jeju National University Graduate School		Convergence Information Security Cooperative Course	6
Joongbu University Graduate School of Humanities Industry		Department of Information Security	9
Chung-ang University	Graduate School	Department of Convergence Security	54
	Graduate School of Security	Department of Industrial Convergence Security	48
Chungbuk National University Graduate School		Convergence Security Interdisciplinary Course	8
KAIST Graduate School		Graduate School of Information Security	61
Hansei University Graduate School of Engineering		Department of Industrial Security and Safety	Newly Established
Hanyang University Graduate School		Department of Information Security	4
Hoseo University Graduate School		Department of Information Security	9
Total		59	1,464

[Source: Higher Education in KOREA, www.academyinfo.go.kr]

Section 3 Professional Curriculum

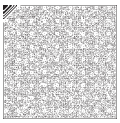
Cybersecurity manpower training programs are divided into public/private sectors and government support projects, depending on the target and purpose of education. In the public sector, education on cybersecurity is being conducted for administrative agencies and cybersecurity officers of their affiliated organizations. In the private sector, industry-tailored long- and short-term courses, such as certification acquisition process and short-term training that reflects industry needs, are provided to the public. Moreover, the government is promoting cybersecurity personnel training programs with professional organizations such as the Korea Internet & Security Agency(KISA).

1. Public sector

The Cybersecurity Training and Exercise Center of the National Security Research Institute (NSR) was opened in October 2014 to strengthen cybersecurity in the national and public sectors by providing practical and field education tailored for information security, and hands-on cyber crisis response training for public institutions and infrastructure officials in charge of computers and security. The curriculum is divided into 'policy, 'introduction, 'prevention, 'detection', and 'investigation'.

Table 3-3-3-1 Annual training course of 2021 Cybersecurity Training and Exercise Center

Sector	Curriculum	Trainees targeted
Policy (3)	Understanding information security work	cybersecurity officers of national and public institutions
	Cybersecurity policy	Central administrative agency administrator levels and subsidiary headquarters manager level
	Infrastructure Security Policy	Central administrative agency manager level and major information and communication infrastructure related organizations manager level
Introduction (5)	Information system establishment and operation Utilization of commercial encryption modulesecure software development	cybersecurity officers of national and public institutions
	Introduction of informatization business security review	cybersecurity officers of national and public institutions
	Security Conformity Verification	Person in charge of introducing, verifying, and operating information security products and network equipment security conformity



Sector	Curriculum	Trainees targeted
Introduction (5)	Utilization of commercial encryption module	cybersecurity officers of national and public institutions
	Development of secure software	cybersecurity officers of national and public institutions
Prevention (5)	Cases of national and public institution security threats	cybersecurity officers of national and public institutions
	Enhancement of office PC security	cybersecurity officers of national and public institutions
	Infrastructure control system security	Infrastructure control system operation officers of national and public institutions
	electromagnetic security	Major information and communications infrastructure-related officers and cybersecurity officers of national and public institutions
	Information security management status evaluation	cybersecurity Management Status officers of national and public institutions
Detection (5)	Cyber crisis response map exercise	cybersecurity officers of national and public institutions
	Malware analysis	cybersecurity officers of national and public institutions
	Malware behavior analysis	cybersecurity officers of national and public institutions
	Security control and incident response	National security control center operation and related workers
	Infrastructure cyberattack response	Major information and communications infrastructure-related officers and cybersecurity officers of national and public institutions
Investigation (4)	Office PC Intrusion Accident Analysis Process	cybersecurity officers of national and public institutions
	Web server breach analysis process	cybersecurity officers of national and public institutions
	Digital Forensics Course	cybersecurity officers of national and public institutions
	Windows Forensics Course	cybersecurity officers of national and public institutions

[Source: Cybersecurity Training and Exercise Center, www.cstec.kr]

The National Human Resources Development Institute, which oversees affairs related to education and training, research and development and evaluation, exchange and cooperation, et cetera, was launched on January 1, 2016, located in Jincheon-gun, Chungcheongbuk-do, as a member of the Ministry of Personnel Management. The National Human Resources Development Institute operates a variety of training

courses - basic education, government philosophy public service posture, public service leadership education, global education, job education, e-learning, et cetera, to strengthen the job competency of government officers. It also provides cybersecurity-related training within the IT training as one of the job training.

Table 3-3-3-2 Information security curriculum of National Human Resources Development Institute in 2021

Sector		Curriculum	Trainees targeted
Information security	Introduction	Getting acquainted with information security	National and local government officers
	Normal	IoT security in everyday life	
		Protecting PC and smartphone information	
		Personal information security practice	
		Information security policy practice	
		Understanding TCP/IP networks	
	Specialty	Network hacking and security	
		System hacking and security	
		Cybersecurity system operation and security	

[Source: National Human Resources Development Institute, www.nhi.go.kr]

2. Private sector

As security issues spread to all industries due to changes in the ICT environment and convergence, long and short-term education courses related to cybersecurity in the private sector have been opened based on various types of demand, from existing education focused on obtaining certificates to education customized to industries.

Training for obtaining a certificate includes Certified Information Systems Auditor (CISA), Certified Information System Security Professional (CISSP), and Certified Information Security Manager (CISM). Since the enforcement of the 「Personal Information Protection Act」, interest in the certificate of the Certified Privacy Protection General (CPPG) has increased, and related certificate acquisition courses have also been opened and operated by several educational institutions.

As industry-specific training courses, job-tailored training such as cybersecurity consultants, security monitoring, and penetration tests is in operation.

Table 3-3-3-3 Private education centers and curriculum in 2021

Organization	Curriculum	Homepage
Korea Information Technology Research Institute	Courses for security incident response, penetration test, security developer courses, etc. Training courses for incumbents and job seekers, etc.	www.kitri.re.kr
Wiseroad	CISSP, CISA, CPPG, information security (industrial) engineer certification course, etc.	wiseroad.co.kr
Lyzeum	CISSP, CISA, CISM, CPPG, information security (industrial) engineer certification course, etc.	www.lyzeum.com
Multicampus	Cybersecurity, CISSP, CISA, information security (industrial) engineer certification course, etc.	www.multicampus.com
Soldesk	Corporate security expert course, penetration testing course, etc.	soldesk.com
KG ITbank	Network/system hacking security expert course, web hacking, forensic (incident response) course, etc.	kgitbank.co.kr
Insec Security	Digital & mobile forensics, security incident analysis, vulnerability assessment, APT attack response network security, etc.	www.traingtotal.co.kr
Fast Lane	Network/mobile/system security course, CISSP, CISA certification course, etc.	www.flane.co.kr
Korea Information Security Education Center (KISEC)	Penetration testing, diagnosis, forensics (intrusion incident), general security process, etc.	www.kisec.com

[Source: Websites by organization]

3. Government-supported cybersecurity training programs

Cybersecurity professional training programs supported by the government include cybersecurity specialized college by the Ministry of Science and ICT (MSIT), Korea University Clubs Information Security (KUCIS), convergence security core talent training program (Convergence Security Graduate School), BoB (Best of the Best), and cybersecurity workforce training (K-Shield Junior) programs. Ministry of Employment and Labor also supports programs to foster top-notch cybersecurity professionals and industrial security experts.

A. Programs of Korea Internet & Security Agency

The Cybersecurity Human Resources Center in KISA has cybersecurity manpower

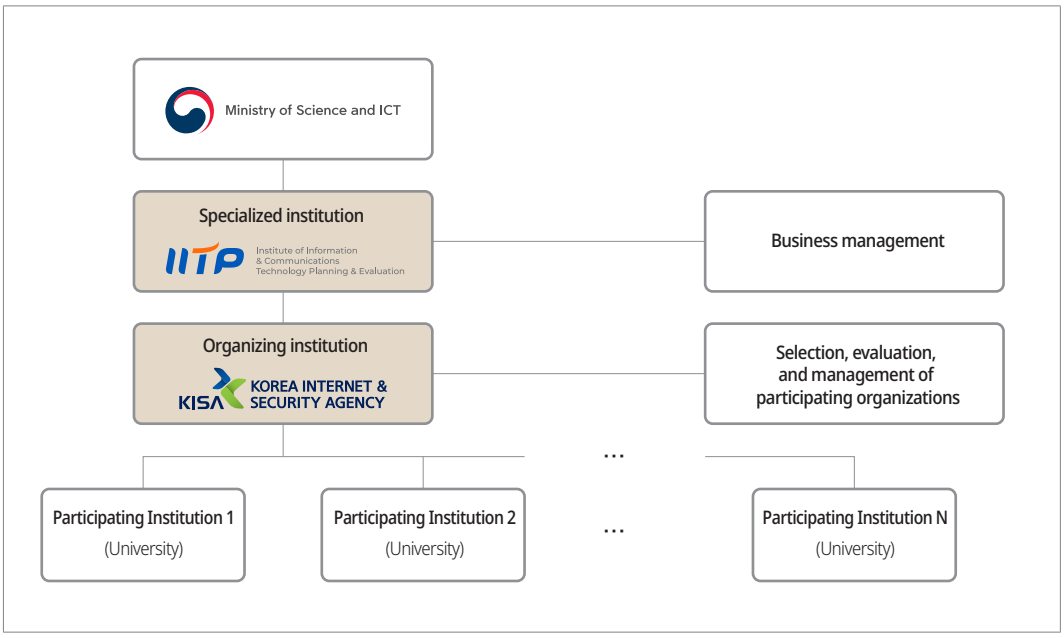
training programs to foster a cybersecurity workforce that will raise global competitiveness and create an educational ecosystem. The center raises the competence of cybersecurity personnel through the elite cybersecurity manpower program, K-Shield, and the industrial security experts training program. Also, the center produces 3,000 and more outstanding human resources every year through customized life cycle education, such as fostering prospective manpower through cybersecurity specialized universities, convergence security core talent training programs, and the university cybersecurity club association.

1) Cybersecurity specialized college

In 2015, the MSIT launched a new project that supports cybersecurity specialized colleges with the KISA for the departments that have cybersecurity specialized curricula. Through this project, universities open a cybersecurity course in the department that reflects the demands of the industry and provides intensive education specialized for cybersecurity tasks.

Korea University, Ajou University, and Seoul Women's University were first selected in 2015, and currently, three universities [Korea University (Sejong), Chungbuk National University, and Sejong University] are operating cybersecurity specialized courses.

Figure 3-3-3-1 Cybersecurity specialized university support project



This program is operated mainly by a consortium composed of participating universities, local and international cybersecurity companies, and universities abroad. It is evaluated as a program to discover and foster outstanding talents for the industry, as it essentially includes the implementation of industry-academic cooperation projects with a consortium of participating companies and the use of professors who are oriented toward industry-academia cooperation. In addition, this contributes to 'entering a cybersecurity university without worrying about the Korean CSAT (College Scholastic Ability Test)' by introducing selection criteria for cybersecurity specialists in connection with the entrance examination process for new students.

2) Nurturing core talents for convergence security (Graduate School of Convergence Security)

The MSIT designates the graduate school of convergence security through a program to foster core talents in convergence security.

Through this program, universities formed a consortium with institutions related to regional strategic industries to open a graduate school of convergence security. The program utilizes problem-solving-type projects to improve the security of ICT convergence products and services in regional strategic industries. Universities are

expected to cultivate convergence security consultants and developers through training in connection with the field and support the convergence of regional strategic industries.

The MSIT selected Korea University in 2019 in the smart factory industry, Chonnam National University in the new energy business, and Korea Advanced Institute of Science and Technology (KAIST) in the smart city industry. 5 additional universities were selected in 2020: Sungkyunkwan University, Kangwon National University, Soonchunhyang University, Pusan National University, and Chungnam National University, focusing on the 5G+ core service industry. To date, there are 8 convergence security graduate schools nationwide.

Table 3-3-3-4 Graduate school of convergence security in 2021

University	Related Industry	Selected in
Korea University	Smart factories	2019
KAIST	Smart cities	
Cheonnam Nation University	New energy businesses	
Sungkyungkwan University	Digital health care	2020

University	Related Industry	Selected in
Soonchunhyang University	Self-driving card	2020
Pusan National University	Fintech	
Digital health care	Digital health care	
Chungnam National University	Smart cities	

3) Korea University Clubs Information Security (KUCIS)

Korea University Clubs Information Security (KUCIS) formed in 2006 has supported cybersecurity education, seminars, and research activities for a person who has cybersecurity and related majors can advance into society with ethical awareness and security capabilities.

In 2021, KUCIS selected 24 clubs which are in colleges, universities, and graduate schools, and supported cybersecurity seminars for information exchange and networking among members, employment and start-up camps, and research activities with the management teams in 4 regions: Seoul/Gyeonggi/Gangwon, Yeongnam, Chungcheong, and Honam.

Table 3-3-3-5 Cybersecurity clubs in universities in 2021

University	Club	Region
Kyonggi University	C-Lab	Seoul, Gyeonggi, Gangwon
	K.knock	
Kyungbok University	SeaHawk	
Kookmin University	FaS	
	PEPSI	
Dankook University	Aegis	
Seoul Women's University	SWING	
	SWLUG	
Sungkonghoe University	DEBUG	
Ajou University	Whois	
Kyungil University	K-Hackers	Yeongnam
Pukyong National University	CERT-IS	
Yeungnam University College	YESS	Yeongnam
Far East University	P.O.S.	Chungcheong
Baekseok University	HUB	
Soonchunhyang University	SecurityFirst	
Cheongju University	CUHA	
Chungnam National University	ARGOS	
Hoseo University	HAIS	
Mokpo University	SecuMaster	Honam
Woosuk University	APS	
Chonnam National University	Cybersecurity 119	
Chosun University	HackerLogin	
Howon University	SEED	

4) Next-generation security leader training program

The Korea Information Technology Research Institute (KITRI) has the BoB (Best of the Best), which is a major information security human resources development program that discovers and nurtures young people - high school, university, and graduate school students who are talented in information security to foster next-generation security leaders with creative problem-solving capabilities.

The BoB, which reached its 8th term in 2019 and expanded the recruitment quota to 200, is renowned for its step-by-step mentoring by the best local and international security experts, practical projects, evaluation and certification of excellent talents, and support for graduates entering society. The BoB, which started with 60 people in its 1st period, has produced a total of 1,490 trainees by the 10th period(2021), and the top 10 trainees selected through the three-level curriculum for each period are awarded the BEST 10 certificate by the Minister of Science and ICT.

5) Convergence Security Manpower Training

To cope with the security threats that spread to various fields due to changes in the ICT environment and convergence, the convergence security curriculum has been provided since 2016 to developers related to ICT convergence products and services.

In 2016, the 'IoT security coordinator course', and the 'IoT device security course' in 2017 were opened and reorganized in 2018 into a curriculum for the ICT convergence industry, e.g., smart energy, smart medical care, and smart home/home appliances. A total of 5 training courses are being operated as of 2021 by adding courses in the field of smart cars in 2019 and smart manufacturing in 2020.

Table 3-3-3-6 Contents of training course for convergence security manpower in 2021

Subject	Training content
Smart energy	Analysis of power plant hacking incidents and vulnerability assessments using virtual power plant environment and training on countermeasures (using Openplc, ScadaBR)
Smart manufacturing	Analysis of smart factory hacking incident and vulnerability assessments using a virtual production facility environment and training on countermeasures (using Openplc, ScadaBR)
Smart medical care	Hacking incident analysis for general hospital, and vulnerability analysis and response strategy for medical devices (using Arduino and wireless LAN)
Smart home appliance	Vulnerability analysis and response strategy in service aspect using home appliances (AI speakers) (using AI Makers Kit)
Smart car	Analysis of smart car hacking incidents and vulnerability analysis and response strategy using virtual smart car environment (using Arduino, vehicle data set)

6) Cyber Range

The cyber range (Security-Gym) in Pangyo Information Security Cluster in Gyeonggi-do has 3 training courses: the team-based one-way security incident response with reproduced the real cases in a virtual environment, the two-way red and blue team exercise for offense and defense, and the security product group training for how to respond against bypassing attack exploiting commercial security products.

In 2017, through pilot training for security personnel in the public sector such as the military and police, 250 graduates were produced. In 2018, the trainee group was expanded to the private sector such as telecommunications companies and financial sectors, producing 357 graduates. Moreover, a lecture-style one-way incident response

course and a beginner-level cybersecurity product group training course were additionally opened for level-specific training, and 382 graduates were produced in 2019.

In 2020, advanced offline training courses focused on major information and communications infrastructure developed in 2019 were opened, and an online training course based on a lecture-style one-way incident response course was opened, producing 1,016 graduates. And, in 2021, it produced 883 graduates.

7) Fostering a cybersecurity workforce (K-Shield Junior)

The MSIT launched the 'K-Shield Junior' curriculum to train job seekers in the field of cybersecurity by benchmarking the 'K-Shield' curriculum for incumbent workers that are well-accepted in the industry as part of the youth job support. The 'K-Shield Junior' curriculum produced a total of 1,371 workforces, starting with 204 students in the 1st semester in 2018 and reaching 358 students in the 7th in 2021.

This course developed a curriculum for each job of 200 hours or more based on 33 competency units and learning modules in the cybersecurity field which is defined in the National Competency Standards (NCS) to foster practical talents who can be immediately committed to the cybersecurity industry and built a dedicated training center. The curriculum is managed by private educational institutions: Culture Makers (CM) and the Korea Information Security Education Center (KISEC). After completion of the training, the K-Shield Junior Certificate by the Minister of Science and ICT is issued to the most talented person through the final evaluation conducted by the KISA.

In addition, as the KISA signed a business agreement (MOU) with 62 companies in 2020 and 73 companies requiring cybersecurity personnel in 2021 to foster excellent manpower and support employment for graduates, the partner companies participate in the development and operation of the curriculum and provide benefits such as special recruitment and preferential employment for the graduates.

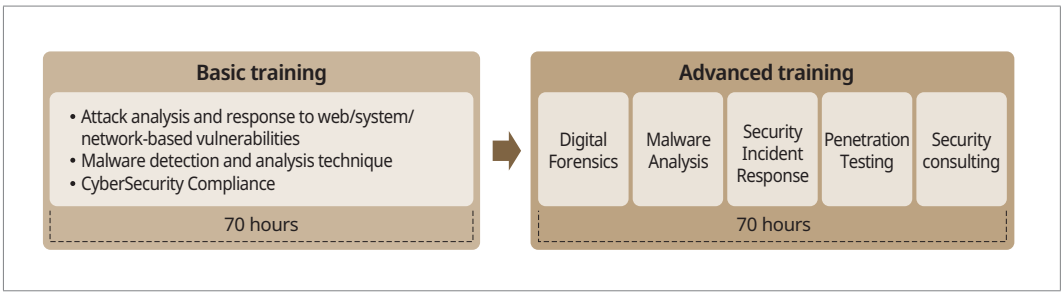
8) Nurturing the top cybersecurity workforce

Since 2013, the KISA has had a program to foster top of a line cybersecurity workforce (K-Shield) to quickly respond to a national cyber crisis such as the cyberattack which took place on 20 March 2013. In this program, practical training is conducted to enhance techniques to respond to security incidents such as vulnerability

and malicious code analysis, and penetration testing. The program is expanded to cover overall security in 2018, cultivating a top-notch cybersecurity workforce to respond against diverse cyberattacks.

Trainees are selected through pre-evaluation conducted for private companies and security personnel in public institutions. The trainees complete the 1st basic training by the common curriculum and then choose one of the five courses: security incidents response, malware analysis, and so on, and take the 2nd training with the advanced curriculum. In 2021, 77 elite cybersecurity personnel were awarded the K-Shield certificates.

Figure 3-3-3-2 K-shield training course in 2021



Existing workforces who have the K-Shield certificate are active by joining the cybersecurity specialist group, and programs are constantly being reviewed that will contribute to national cybersecurity capacity building, e.g., mentoring in the cybersecurity field and connecting with private companies.

9) Nurturing security experts for industry

In order to foster field-oriented working talent and to improve the qualitative supply and demand gap of the industrial workforce, the KISA produced 260 graduates in 2009, by reflecting each industry's required competencies and opening four training courses, including digital forensics with enhanced practice, knowledge and information security consultants, RFID/USN security, and biometrics.

Table 3-3-3-7 2021 industrial security professional training course

Course	No. of openings	Training hours
Incident response and analysis expert	3	28
Secure coding to defend against hacking	4	21
Network Security Theory and Practice	3	28
Digital forensic practice	2	28
Practical application of encryption and authentication	2	21
Web hackings and countermeasures	3	21
Security consulting theory and practice	3	21
Infrastructure cybersecurity business practice	3	28
Control system security	3	28
Container Security in DevOps Environments	2	21
Cloud Security Implementation Practice	2	21

In 2011, the KISA added security monitoring and information security skill-up courses by industrial demand and later integrated them into the program of the Ministry of Employment and Labor's consortium for the HRD magnified program in 2012 in the process of integrating workforce training programs from each ministry.

In 2021, the program of work on education is established by collecting opinions from the industry and experts from the academy, with 11 curriculums such as 'Expert on infringement incident analysis and response', 'Secure coding for hacking defense', etc.

10) Training manpower for AI security technology development

The MSIT and the KISA have a training course for professionals with the ability to develop intelligent security technologies using AI from 2020 to support innovation in automation technology and intelligent technology for cybersecurity. In the first AI security technology development training sessions in 2020, 50 graduates were produced, and 5 excellent trainees were selected and awarded certificates by the President of the KISA.

Besides, they promote employment support such as job counseling, employment consulting, and employment information for unemployed trainees to provide employment opportunities for trainees and to meet the demand for professional manpower in the industry.

AI security technology development training is organized to complete specialized training focused on AI technology application practice in each industry sector after completing the common education consisting of prerequisite courses based on theory. In 2021, they conducted intensive practical training in three areas: attack and defense using AI and user authentication, security log analysis and anomaly detection and analysis, and intrusion detection through data analysis. After taking the training, they conducted a project on new AI security technology development to check and share the outcome of the training.

B. University ICT Research Center (cybersecurity field)

The University ICT Research Center (ITRC) has been supported by the MSIT and the Institute of Information & Communications Technology Planning & Evaluation for the purpose of fostering professional researchers at the master's and doctoral levels with advanced research capabilities since 2000. From 2000 to 2020, the ITRC contributed to the creation of new growth power and new industries by producing 15,841 talents, 5,359 patent registrations, about 48.1 billion KRW in technology transfer income, and 12,602 SCI-level papers.

In 2020, a total of 51 research centers received support, and among them, the ITRC in the field of cybersecurity is operated by the Artificial Intelligence Security Research Center of Soongsil University.

C. National Infrastructure and strategic industry job training (cybersecurity experts)

'Job Training Programs for National infrastructure and Strategic Industries of the Central Government' is managed by the MSIT and the Ministry of Employment and Labor and run by the Korea Information Technology Research Institute. This project is being operated with to produce recruits in the information security industry through long-term (5+ months) specialized technical training for the unemployed who wish to enter the information security industry.

This program can be participated by applying and issuing a vocational competency development account managed by the Ministry of Employment and Labor. Participants may be subject to receiving full support for tuition fees and additional support for meals and transportation expenses.

Table 3-3-3-8 **Training courses for national mainstay and strategic industries of the Central Ministries in 2021**

Trainee	Course	Capacity
Job seeker	Training course of incident response expert	270 persons
	Training course of penetration testing experts	
	Training course for corporate recruitment	
	Training course for security developers	
Incumbent	Training course for CISO	

D. Curriculum by the Financial Security Institute

1) Cyber education

The Financial Security Institute provides customized cyber education through the Financial Security Education Center (edu.fsec.or.kr) to raise the level of cybersecurity awareness of financial company employees and to cultivate job skills necessary for financial IT changes. In particular, in 2021, the Financial Security Institute provided a micro-learning* course consisting of short content centered on key points so that people can easily take it anytime, anywhere.

* Micro-Learning: One-point education consisting of short content centered on the key points (e.g., TED, Knowledge of the Channel e, etc.)

Table 3-3-3-9 **Cyber curriculum in 2021**

Field	Course
Basic knowledge (17)	Basic duty in a non-face-to-face work environment
	Understanding of MyData in the Financial Industry
	Revisions to the Data 3 Act and Notes on its Application to the Financial Industry
Basic knowledge (17)	Digital financial security issues (including English courses)
	Understanding networking fundamentals
	Understanding of financial security laws and systems
	Impact of the 4th Industrial Revolution and security threats and responses
	Analysis of electronic financial services according to changes in the financial environment
	Raising awareness of cybersecurity
	Secure electronic financial transaction

Field	Course
Basic knowledge (17)	Understanding financial security governance
	Understanding of financial IT internal audit activities
	Introduction to Financial Security for new employees
	Prospects of financial security threats
	Types of recent cyberattacks in the financial sector and responses
	IT Outsourcing Company Security A to Z
	Considerations when introducing the financial sector cloud system
Job basics (10)	Financial sector APT attacks and countermeasures
	Financial data analysis practice using AI
	Financial environment and issues in the blockchain
	Cryptographic technology for safe financial security
	Understanding of electronic financial security authentication technology
	Basics of cybersecurity compliance and system management
	Financial security for counselors
	IT outsourcing and financial security
	Financial IT internal control with required compliance for financial company executives and employees (including English language courses)
	Self-level diagnosis and compliance matters to prevent leakage of internal information
Job reinforcement (11)	Cases of IT security violations in the financial sector
	Dark Web and Open Source Intelligence (OSINT)
	Financial cloud introduction and security
	Establishment and use of an information security management system (including English language courses)
	Understanding secure coding for safe software
	Understanding Windows system security
Job reinforcement (11)	Personal (credit) information protection
	Personal information protection in the financial sector for those in charge of personal information
	Financial sector personal information protection for personal information trustees
	Financial sector personal information protection for personal information handlers
	Threats and responses to financial IT security

2) Group education

To provide professional and in-depth education, security officers in the financial sector are classified by class, such as C-Level, manager, and working-level officials, and a group training course specialized for each class is being operated. As the COVID-19 situation continues, in 2021, various non-face-to-face education channels (YouTube, Zoom, etc.) were used to operate the curriculum flexibly. Also, to maximize the effect of group education, a flip learning* course was provided.

* Flipped Learning: Blended learning in which individual learning is conducted online in advance and then practice and discussion are conducted offline

Table 3-3-3-10 Major group education in 2021

Course	Target of education	Operation type
Financial cybersecurity and personal information protection management system	Managers· Practitioners	Theory
Financial IT Compliance		
Cybersecurity strategy establishment and management measures		
Financial IT audit practice		
Understanding the legal system related to financial cybersecurity		
Personal information protection in the financial sector	Practitioners	
Fundamental of personal information protection commission and entrustment work in the financial sector		
Personal credit information protection in the financial sector		
Response to Digital New Deal and Financial Cyber Threats		
ISMS-P certification evaluation practice		
The present and future of financial mobile malware		
Impact of the enactment of the Data Framework Act (draft) to promote data transactions and utilization on the financial sector		
What the Data Framework Act means to the financial industry		
Safety evaluation criteria and methods for cloud computing service providers in the financial sector		
Metaverse financial sector use cases and security issues		
Personal (credit) information protection practice related to the consignment business of the financial sector		
Financial IT cloud security technology		Practice
Cloud security service operation practice		
Utilization of financial data analysis		

Course	Target of education	Operation type
Financial data pseudonymization and anonymity processing and utilization	Practitioners	Practice
Understanding the financial sector vulnerability inspection methodology		
Android mobile app vulnerability analysis		
Fostering dedicated financial security personnel		
Financial system development security		
Financial app malware reversing		
Analysis and Response to Financial Infringement Incidents		
Financial APT Attacks and Responses		
Cybersecurity system operation and management practices		
Windows system malware detection and response		
In-depth analysis of document file malware		
Cloud security management achieved with DevSecOps		
Introduction to Financial IT Security		
Financial security data analysis using AI		
Practice using AI-based data analysis		
Digital Forensics Fundamentals		
Practice! Web hacking and reversing (latest CTF problem solving)		
Python web crawling to collect financial and security information		
Intrusion prevention self-inspection tool user training		
Implementation of blockchain platform using Ethereum		
Introduction of vulnerability management tools in financial sector based on evaluation criteria for electronic financial infrastructure		
5th financial security C-level course	CISO etc.	
Training of financial CISO security leaders	CISO	

3) Certified Financial Security Expert (CFSE) qualification system

Since 2018, the Financial Security Institute has been implementing a Certified Financial Security Expert (CFSE) qualification system linked to the professional training courses on financial information security-related laws and systems, management systems, and financial IT security in order to cultivate verified security experts necessary for the financial sector. In accordance with the spread of COVID-19, the professional training courses have been converted to online education, creating an environment for non-face-to-face education. In order to provide more opportunities for employees of

financial companies to take the exam, the qualification test has been expanded from once a year to twice a year, making efforts to nurture financial security experts.

The Certified Financial Security Expert (CFSE) qualification system is a private qualification registered under the jurisdiction of the Financial Services Commission and consists of a professional training course and qualification test. So far, a total of 150 financial security managers were produced: 29 in 2018, 33 in 2019, 29 in 2020, and 59 in 2021. And, 436 people participated in the training by 2021.

4) Financial security camp

With the Financial Information Security Association and the Financial Security Forum, the Financial Security Institute co-hosts a financial security camp in which university (graduate) students from all over the country participate in support of fostering future financial security personnel. In 2021, they held an online financial security camp due to the spread of COVID-19, and 88 undergraduate (graduate) students from 39 universities participated.

Section 4 Competitions

As the need for cybersecurity has greatly expanded due to changes in the Internet use environment, online infringement incidents have been on the rise. Due to the increasing cyber infringement incidents, the need for information protection grows, and consequently, the training of professional manpower is emerging as a new issue. The government and major organizations are therefore holding various hacking defense competitions as part of efforts to discover and foster information security experts and raise awareness of cybersecurity. The main competitions held in Korea in 2021 are as follows.

1. Cyber Conflict Exercise

The 2020 Cyber Conflict Exercise, hosted by the National Intelligence Service (NIS) and organized by the National Security Research Institute (NSR), was held online from

September 3 to October 27. This competition has been held since 2017 to enhance crisis response capabilities in the event of a national disaster caused by a large-scale cyberattack. In this competition, participants in the national, public, and private sectors can experience cyberattacks similar to real-life to improve cybersecurity capabilities. In addition, the competition is operated as a complex capacity-building training that evaluates communication skills during a cyber crisis along with technical response skills.

2. CODEGATE

CODEGATE, which started in 2008, is the first international hacking defense contest in Korea and is being operated by the CODEGATE Security Forum. This competition is held once a year as a global information security event to explore new information security technologies by capturing the trends of the 4th industrial revolution centered on IT and sharing inspiration for trends.

In the 2020 competition, 735 teams from 58 countries participated in the general division, 618 local teams participated in the college student division, and 309 people from 43 countries participated in the junior division. In the general competition, the United States' 'PPP' team won the championship, and Korea's 'Yangjinmotti' team, which had won the championship twice in a row, finished in second place. In addition, Korea University's 'Cykor' team won the college student division and Lee Jin-heon of Sunrin Internet High School won the junior division.

The 2021 CODEGATE competition was canceled due to the spread of COVID-19 and is scheduled to be held in 2022.

3. Hack the Challenge

The KISA is holding the 'K-Cyber Security Challenge', a competition that uses Artificial Intelligence (AI) and big data to compete for intelligent security technology and its performance. As part of the challenge, the KISA held 'Hack the Challenge 2021' with 8 private companies including Naver, Mobizen, Samsung SDS, Shinsegae DF Co., Ltd., INCA Internet, SR Co., Ltd, NCsoft, and Jiran Security to find vulnerabilities in homepages, corporate solutions, and IoT devices in action. A total of 595 people

participated in the competition and reported 689 cases, of which 217 were found to be effective vulnerabilities. The number of participating companies in the competition was expanded from 5 to 8, and the field of vulnerability discovery was expanded from the existing websites to a virtual environment where enterprise solutions were installed on the competition platform.

However, despite the continued occurrence of homepage defacement and personal information breach incidents by exploiting homepage vulnerabilities, the discovery of homepage vulnerabilities was considered illegal according to the law. For this reason, there was a limit to discovering website vulnerabilities for public interest purposes.

Thus, in 2018, the KISA opened the five sites in operation and held the 'Hack the KISA' contest for the first time as a public institution to discover vulnerabilities through penetration testing by private security experts. A total of 485 people participated in the competition to discover and report 163 vulnerabilities, and a total of 25.55 million KRW was awarded for 60 effective vulnerabilities. Among the valid vulnerabilities, some of them are not identifiable by common security inspection tools, which emphasized the importance of the contest.

In addition, in 'Hack the Challenge' in 2019, in cooperation with the three companies Naver, RIDI, and Soteria, the target of vulnerabilities was expanded to not only the homepage operated by the KISA but also the homepage operated by the company. A total of 126 people participated and reported 465 cases, and 46 valid vulnerabilities were found. Therefore, the event proved that the collaboration with private companies' security experts enables the discovery of the service vulnerabilities stably.

The 'Hack the Challenge' model can contribute not only to preventing hacking of the company's website but also to improving the level of cybersecurity across the country. In the future, the KISA, therefore, plans to actively support the introduction of a vulnerability discovery model for the homepages operated by domestic companies.

4. Cybersecurity Thesis Contest

The Cybersecurity Thesis Contest is a competition for fostering future talents hosted by the National Intelligence Service (NIS) and supervised by the Korea

Institute of Information Security & Cryptology and the Korean Association of World Politics of Information.

The '2021 Cybersecurity Thesis Contest' is a contest for research in all fields of technology and policy. The scope of the competition is comprehensive, including system security, network security, convergence security/industrial security, law, policy, and national strategy, but applicants are limited to undergraduate (graduate) students. The total prize is 31 million KRW, and a total of 20 titles have been awarded, including the Grand Prize and the Excellence Prize, and excellent papers were recommended to be published in the journals of the Korea Institute of Information Security & Cryptology and the journals of the Korean Association of World Politics of Information, if desired.

5. National Cryptography Competition

The National Cryptography Competition is for the development of cryptographic technology hosted by the KISA and the NSR, organized by the Korea Cryptography Forum and the Korea Institute of Information Security & Cryptology, and sponsored by the NIS. In the 2021 National Cryptography Competition, a total of 72 teams submitted 47 papers in the field of cryptographic theory and cryptographic application. Through the first written examination and the second in-depth interview, the judging committee, made up of academic experts, selected a total of 31 teams as the final award winners, including 16 teams in the theory field and 15 teams in the application field. The Grand Prize was awarded to the Kookmin University team that analyzed the safety of hash functions based on symmetric-key cryptography (AES-256) in a quantum computer environment, and the Excellence Prize was awarded to the Korea Advanced Institute of Science and Technology, Seoul National University, Korea University, and Hanyang University.

6. Cybersecurity Academy

The '2021 Cybersecurity Academy for Undergraduate (Graduate) Students' hosted by the NIS, the NSR, and the International Cyber Law Studies, and organized by the Korea University Cyber Law Centre, was held in August. This is an educational program aimed at raising awareness of cybersecurity, which started with the 'Cybersecurity

Academy for Undergraduate (Graduate) Students' in 2014 hosted by the NSR and Korea University Law School.

The education in 2021 provided an opportunity to understand basic knowledge and current issues related to cybersecurity, such as concepts of cybersecurity, major threats, and norms, to undergraduate (graduate) students in various majors. In particular, through lectures by executives from major security companies, practical information such as demand, prospects, and directions of future field security personnel was delivered to students. In 2021, 150 students were issued a certificate under the joint name of the Director of the National Cyber Security Center, the President of the NSR, and the President of the International Cyber Law Studies.

7. Financial Security Institute Thesis Contest

The Financial Security Institute has held a thesis contest every year since 2017 for those working in the financial field, university (graduate) students, and the general public to discover excellent theses in the field of digital financial innovation and financial security.

A total of 49 papers were submitted to the 5th Financial Security Institute Thesis Contest in 2021. After an impartial examination, a total of eight films were awarded, including the Grand Prize (The Chairperson of the Financial Services Commission Award) and the Excellence Prize (Governor of the Financial Supervisory Service Award).

Section 5 Cybersecurity Certification

As the importance of cybersecurity has emerged and the demand for professional manpower has increased, interest in cybersecurity certification that evaluates cybersecurity theory and practical ability is growing.

Table 3-3-5-1 Cybersecurity Professional Certification

	Title	Classification	Coordinated by
Local	Information security engineer, industrial engineer	Engineer/ Industrial Engineer	MSIT, KISA
	Specialist for Information Security (SIS)	Level 1, Level 2 ※ Maintain qualification	KISA
	Certified Privacy Protection General (CPPG)	-	Korea Chief Privacy Officers' FORUM
	Digital Forensics Expert	Level 1, Level 2	Korean Institute of Forensic Science, KISA
	Industrial Security Expert	-	Ministry of Trade, Industry and Energy, Korean Association for Industrial Technology Security
	Certified Cyber Forensics Professional (CCFP)	-	Korea Cyber Forensic Professional Association
International	Certified Information Systems Security Professional (CISSP)	-	ISC2
	Certified Information Security Manager (CISM)	-	ISACA

1. Cybersecurity professional certification in Korea

A. Information security engineer/industrial engineer

Two new categories of cybersecurity engineer and industrial engineer were set up in 2012 as national technical qualifications in Korea, and the KISA has been the entrusted organization and put into operation since 2013.

Information security engineer/industrial engineer benchmarked the qualification of Specialist for Information Security (SIS), which was a state-recognized private qualification in the past, and has been in effect as a national technical qualification

exam since 2013.

※ Note: Qualification is now discontinued for SIS, however, existing qualification remains valid.

Table 3-3-5-2 Examinees and passers of National Information Security Technical Qualification Exam

Year	Information security engineer			Industrial information security engineer		
	Skill test applicants	Successful applicants	Final acceptance rate	Skill test applicants	Successful applicants	Final acceptance rate
2013	3,187	210	6.6	436	149	34.2
2014	2,558	315	12.3	556	87	15.7
2015	3,853	488	12.7	670	252	37.6
2016	4,144	306	7.4	1,292	247	19.1
2017	5,122	631	12.3	1,456	500	34.3
2018	4,650	805	17.3	1,225	288	23.5
2019	4,336	461	10.6	982	254	25.9
2020	4,372	348	8.0	886	331	37.4
2021	3,956	76	2.0	923	294	31.8
Total	36,178	3,640	10.1	8,426	2,403	28.5

This qualification exam has two tests: written and skill. The written test is objective and has 4 courses of study including system security, network security, application security, and general information security for an industrial engineer, while the engineer has 5 courses to which the course of information security management and legal is added. The skill test is a written reply which has 3 types: short-answer, descriptive, and practical, and has a single course of information security practice that verifies knowledge and skill appropriate for practice.

Information security engineer/industrial engineer exam is semiannual for each written and skill test in 2021, and had 14,848 applicants, and produced 76 engineers and 294 industrial engineers.

Since 2022, the information security engineer/industrial engineer has been supervised by the Korea Communications Agency.

B. Digital Forensics Expert

The Digital Forensic Expert Level 1 exam, which has been implemented since 2016, evaluates problem-solving skills using techniques such as disk analysis, database analysis, network analysis, mobile analysis, and intrusion incident response forensics. Level 2 exam has a written test which has five courses: computer structure and digital storage media, file system and operating system, understanding applications and networks, database, and introduction to digital forensics, and a skill test focused on practical questions in digital forensics.

C. Industrial Security Expert

The industrial security expert exam was approved by the Minister of Trade, Industry and Energy in 2016 and has been implemented as a state-certified private certification since 2017. This qualification aims to cultivate human resources who perform prevention, management, and response tasks so that the targets of protective value in the field, industrial technology-related personnel/management, facilities/areas, and information/documents, are not affected by internal and external risk factors.

The exam is a written test to evaluate the ability to perform comprehensive practical security tasks such as establishing, implementing, and evaluating security policies for technology protection in industrial sites based on theory, basic knowledge, and applied capabilities for each field related to industrial security. The exam has five courses in total: administrative security, physical security, technical security, security incident response, and security knowledge management.

After being elevated its status to a state-recognized private qualification, the exam was conducted 10 times from 2017 to 2021, producing a total of 1,547 successful candidates.

Table 3-3-5-3 **Examinees and passers of Industrial Security Expert Qualification Test**

Year	Applicants	Successful applicants	Final acceptance rate
2017	1,114	537	48.2
2018	869	306	35.2
2019	752	224	29.8
2020	492	165	33.5
2021	734	315	42.9
Total	3,961	1,547	39

2. International cybersecurity professional license

A. Certified Information Systems Security Professional (CISSP)

Certified Information Systems Security Professional (CISSP) is a certification administered by the International Information Systems Security Certification Consortium, Inc. (ISC2). And, it is the first international certification in the information security industry that meets the strict requirements of ANSI/ISO/IEC 17024. It has produced 150,000 licensees worldwide, and 2,122 are active in Korea. Besides CISSP, ISC2 is in charge of certifications such as CCSP (Certified Cloud Security Professional), SSCP (Systems Security Certified Practitioner), CSSLP (Certified Secure Software Lifecycle Professional), and HCISPP (Healthcare Information Security and Privacy Practitioner).

Table 3-3-5-4 CISSP qualification holders

(Unit of measurement: persons)

	Worldwide	Korea	United States	Japan	China	Hong Kong	Singapore	Australia
Holders	152,632	2,122	94,320	3,339	3,866	1,960	2,804	3,169

The CISSP certification exam evaluates eight domains including security and risk management, security architecture and engineering, and communication and network security. Only those who have fulfilled 5 years or more of work experience in the eight domains are eligible to apply for the exam. However, a person who satisfies certain conditions, such as holding a bachelor's degree or an accredited professional certification, can apply even with work experience of fewer than four years. Even those who do not meet the conditions of experience can receive a formal certification if they meet the conditions after passing the test (Associate program).

B. Certified Cyber Forensic Professional (CCFP)

The Certified Cyber Forensic Professional (CCFP) qualification examines expertise in forensic techniques and procedures, standards of practice, and legal and ethical principles to secure digital evidence that can be recognized in court.

Since 2003, it was only provided as a domestic qualification, but in September 2013, the CCFP qualification was transferred to ISC2 (USA) and was promoted to an

internationally recognized qualification. However, in 2017, the CCFP qualification was repealed by the agreement of the ISC2 executives and the Certificate Policy Committee. And, the qualification was maintained at an internationally recognized qualification until 2020.

Since 2021, the CCFP has been registered and operated as a domestic private qualification. The Cyber Forensic Experts Association (KCFPA) is in charge of the CCFP, evaluating evidence and characteristics, the evidence's chain of custody, enforcement procedures, the role of expert testimony, and the subjects of the Code of Ethics through written or practical methods.

C. Certified Information Security Manager (CISM)

To acquire the CISM (Certified Information Security Manager), at least 5 years of work experience in the field of cybersecurity is required, for which 3 or more years should be in cybersecurity management. There are four evaluation areas: information security governance and information risk management and compliance, information security program development and management, and information security incident management. Globally, it produced 50,043 qualified people, and as of December 2021, 61 people are active in Korea. The CISM qualification test is hosted by the Korea Information Systems Audit and Control Association (http://isaca.or.kr).

3. Certificates related to local and international cybersecurity

Information system supervisors and Certified Information Systems Auditors (CISA) are classified as cybersecurity certifications because they also require security knowledge for qualification.

A. Information System Supervisor

The Information System Supervisor certification is state-certified certification in the field of information and communication supervision, in which the National Information Society Agency (NIA) conducts a qualification examination every year to secure professional manpower to perform information system supervision. This exam is for advanced technicians who have more than 7 years of practical experience after acquiring a professional engineer or engineer certificate or 6 years

or more of practical experience after acquiring a master's degree. It selects successful candidates through a written test consisting of five subjects (supervision and business management, software engineering, database theory, system structure, and security) and an interview screening. After that, two weeks of theoretical education and one week of supervision practical education must be conducted.

B. Certified Information System Auditor (CISA)

Certified Information System Auditor has been managed by the Information Systems Audit and Control Association (ISACA) since 1969. There are 102,887 qualifications worldwide, and 2,302 qualifications are active in Korea as of December 2021. CISA exam includes questions in five areas: information systems auditing process, IT governance and management, information system acquisition, development and implementation, information system operation, maintenance and support, and protection of information assets.

Chapter 4

Personal Information Protection

Section 1

Amendment of the 「Personal Information Protection Act」 and Administration System

1. Amendment of the 「Personal Information Protection Act」

The 「Personal Information Protection Act」 was enacted in March 2011. And, it was revised on February 4, 2020, including the integration of personal information protection-related regulations in individual laws, and came into effect on August 5. The main contents of the current 「Personal Information Protection Act」 are as follows.

The current 「Personal Information Protection Act」 has made the concept of personal information clearer and laid the groundwork for a vigorous use of personal information by introducing the new concept of de-identification. In particular, the regulations on de-identification stipulate that de-identified personal information can be used for statistical purposes, scientific research, etc. without the consent of the data owner. Moreover, regulations related to the protection of personal information in the 「Information and Communications Network Act」 were incorporated as special regulations. Accordingly, information and communications service providers,

like personal information managers, became subject to the 「Personal Information Protection Act」. The Personal Information Protection Commission (PIPC) was upgraded to a central administrative agency (August 5, 2020), strengthening its status as a personal information protection supervisory body.

After the enforcement of the 「Personal Information Protection Act」, there was a recommendation from various fields (industrial circles, legal circles, academia, civic groups, etc.) that it was necessary to further revise the 「Personal Information Protection Act」. First of all, since the 「Personal Information Protection Act」 contains special regulations regarding the processing of personal information by information and communications service providers in addition to the existing personal information managers, the problem of dual regulation on online and offline and aggravation of confusion about offenders was pointed out. Besides, when the Data 3 Act (「Personal Information Protection Act」, 「Information and Communications Network Act」, and 「Credit Information Act」) was revised in February 2020, the issues of 'substantialization of the rights of information subjects in the digital age' and 'improvement of consistency with global norms' were proposed as a next legislative task. Therefore, some pointed out that these matters should also be reflected in the 「Personal Information Protection Act」.

For this reason, the Personal Information Protection Commission (PIPC) started discussing further revisions, such as operating a task force (TF) to amend the 「Personal Information Protection Act」 after its inception (August 5, 2020). In January 2021, the PIPC produced a draft amendment to the 「Personal Information Protection Act」. Afterward, the amendment draft had a gathering of opinions from various fields and expert review, including a meeting with industrial circles and civic groups, an online public hearing, the 4th Regulatory and Institutional Innovation hackathon, consultation with related ministries, and a review by the Regulatory Reform Committee (April 2021). In July 2021, the final amendment to the 「Personal Information Protection Act」 (Government bill) was made. After the cabinet meeting, this government bill was proposed as government legislation on September 28, 2021, and is currently pending in the National Assembly.

The main contents of the amendment to the 「Personal Information Protection Act」 (Government bill) can be categorized as 'preparing the foundation for digital economy growth, strengthening the people's information sovereignty suitable for the

digital age, and ensuring consistency with global regulations', and the detailed main contents are as follows.

Table 3-4-1-1 Main contents of the government bill of Personal Information Protection Act

Type	Major Content
Strengthening the rights of the people suitable for the digital era	• Establishment of a general legal basis for the right to request transmission of personal information (right to move) ※ Currently, only the financial and public sectors are piloted → Free data movement between all sectors and businesses • In cases where automated decisions based on artificial intelligence have a significant impact on the rights and obligations of the people, such as recruitment and selection of welfare recipients, the right to respond positively, such as refusal and request for an explanation, is newly established. • Substantialization of complex and formal 'consent' into a consent system that the public understands ※ Improvement of mandatory consent for contract signing and implementation, the introduction of personal information processing policy evaluation system, etc.
Digital-oriented legal system	• Preparation of operating standards for the safe use of mobile image information processing devices such as drones and autonomous vehicles • Applying the principle of 'same conduct – same regulation' by converting special cases of information and communication service providers into general regulations and reorganizing unreasonable regulations
Ensuring consistency with global regulations	• Conversion of excessive punishment regulations to economic punishment (recommended by the industry) ※ Deleted penalties for personal information collection and use (5 years) and leakage (2 years) → Conversion to fines • Changed the upper limit of penalty surcharge from 'relevant sales' to 'total sales' in line with international standards ※ EU: 4% of global sales, China: 5% of previous year's sales, Canada: 5% of global sales • Diversification of overseas transfer requirements for cross-border data movement, and establishment of an order to suspend overseas transfers for secure data movement

2. Personal Information Protection Administration System

The PIPC is a central administrative agency under the Prime Minister. However, according to the current 「Personal Information Protection Act」, its independence is secured concerning personal information protection matters, in regards to the Articles 7-8 sub-paragraphs 3 and 4 (matters concerning the investigation into infringement upon the right of information subjects and the ensuing dispositions, handling of complaints or remedial procedures relating to personal information handling and mediation of disputes over personal information), and matters of deliberation & resolution under Article 7-9(1) sub-paragraph 1 (matters concerning the assessment

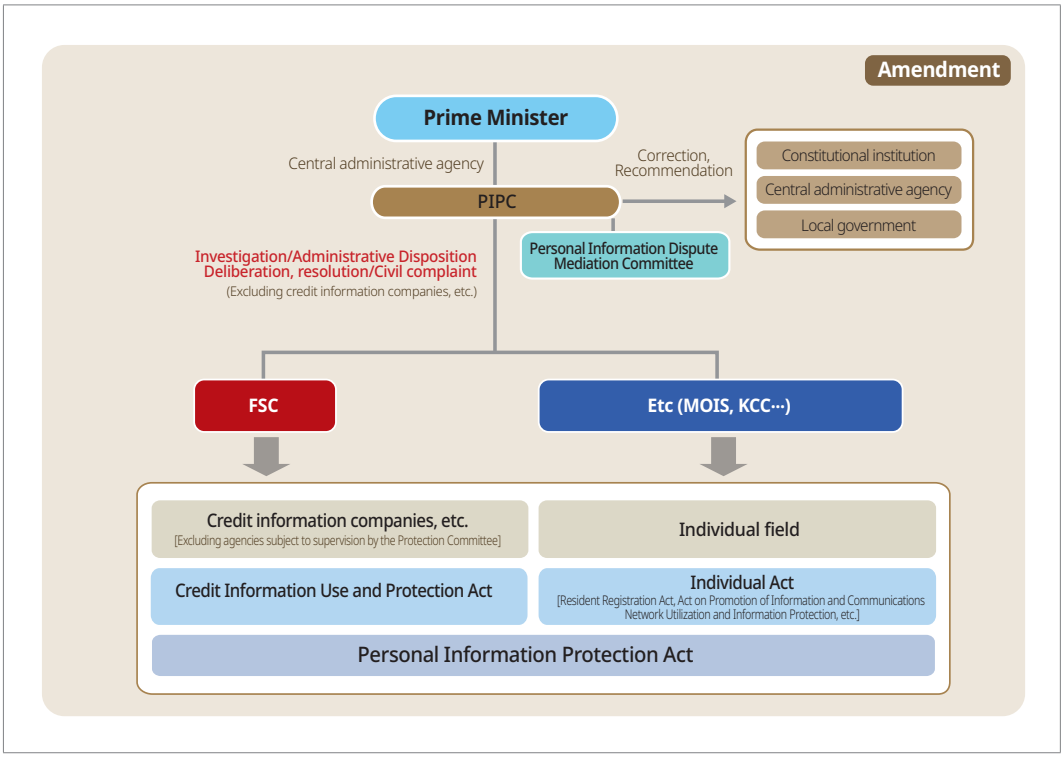
of data breach incident factors), as not being administratively supervised by the prime minister. In addition, as it succeeded the duties of the Ministry of the Interior and Safety (MOIS) and the Korea Communications Commission (KCC), it then carries out the tasks including the establishment of laws and policies related to personal information protection, conducting surveys on personal information protection, requesting data submission and assessment, administrative measures (corrective measures, recommendation for improvement, administrative fines, etc.), and education & public relations of personal information protection. It also provides suggestions to relevant central administrative agencies, recommends improvement of personal information handling status for personal information handlers, operates a personal information infringement report center, and submits and inspects data. Besides, it carries out the registration of personal information files, personal information protection certification, personal information impact assessment, and receipt of the personal information breach report.

Moreover, the PIPC provides recommendations on corrective measures against violations of the law to central administrative agencies, local governments, courts, and constitutional institutions, and set up the 'Personal Information Protection Master Plan' every three years. It also gives recommendations on improvement and performance assessment for policies, regulations, and laws of each agency.

The central administrative agency shall establish an implementation plan for personal information protection in the area under its jurisdiction, and discharge personal information protection duties that fit the purpose of the 「Personal Information Protection Act」.

The central administrative agency shall establish and implement an annual implementation plan for personal information protection by the 'Master Plan'. Public institutions should perform mandatory privacy impact assessments on personal information files with specified sizes or bigger. When operating a visual data processing device in an open place, advice from the experts and stakeholders shall be collected before the installation. Moreover, a signboard on the installation and operation of visual data processing devices shall be set up so that the data owners can be easily aware of data generation.

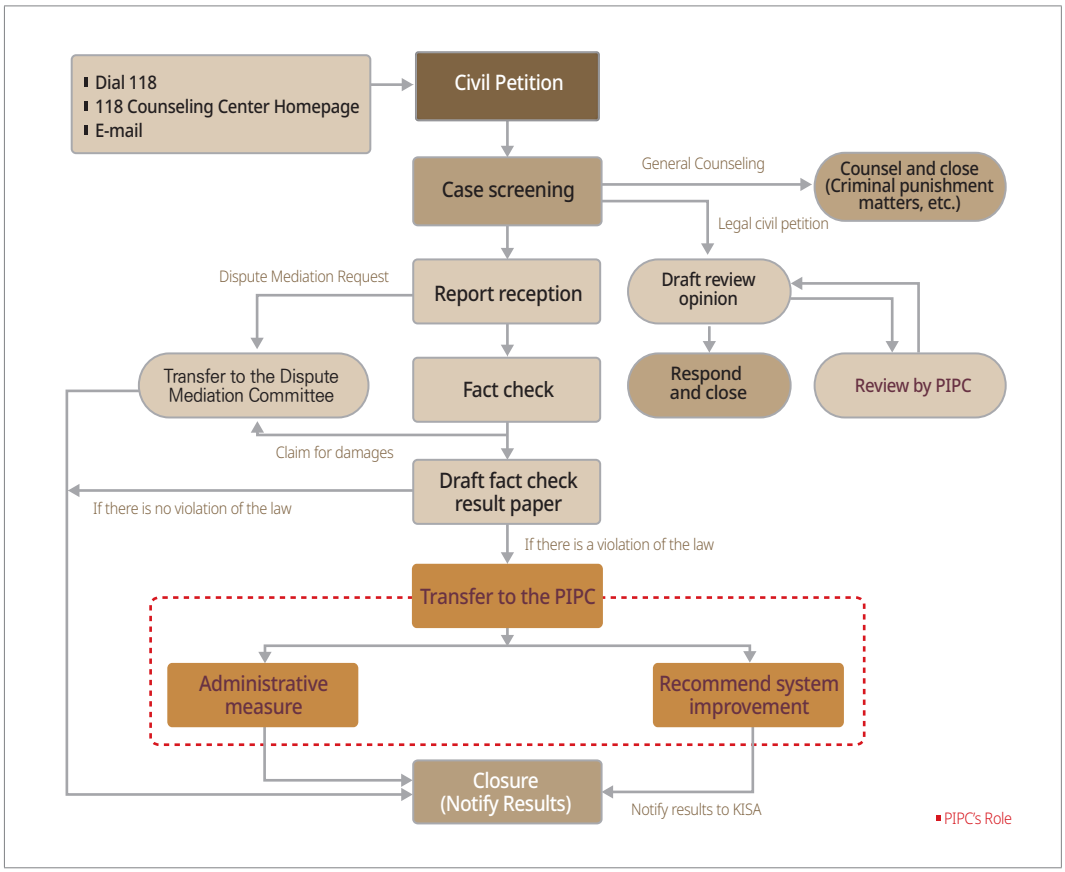
Figure 3-4-1-1 Personal Information Protection Administration System



The data owners may request the right to request access, correction and deletion of personal information, suspension of processing, etc. When the information subject requests such rights, the personal information handlers shall notify the results of the processing to the information subject.

In addition, a person who operates a personal information file for business, not only for public institutions but also for general business operators, associations, organizations, etc. shall prepare or take measures to ensure the protection of data owners' rights.

Figure 3-4-1-2 Reporting procedure on personal information infringement



Section 2 Strengthen Legal Framework

1. Public and General Sector

Even after the 「Personal Information Protection Act」 was enacted, incidents are continued for collection/offer, breach, and misuse/abuse of personal information. Particularly, in January 2014, 88.68 million cases of massive personal information were breached due to a credit card company incident. And, 11.7 million personal information was exposed due to a telecommunication company incident in March of the same year. A local online shopping mall, 'Interpark' incident, which occurred in May 2016 and was reported in July, involved more than 10.3 million members' personal information, resulting in a large-scale incident with more than 10 million cumulative credentials.

In July 2014, the Ministry of Interior and Safety (MOIS), the Korea Communications Commission, the Personal Information Protection Commission, the Financial Services Commission (FSC), and the Ministry of Science and ICT (MSIT) had a joint announcement on the 'measures to reinstate personal information protection', to protect personal information and for system improvement to prevent a recurrence. The measures include seven key tasks, including deployment of the damage compensation program, and tightening penalties for personal information-related crimes. Thereafter related laws and policies are also strengthened.

The 「Personal Information Protection Act」 has kept revised to enhance the personal information protection level. In 2016, the Act mandated to inform the data owner of the data source and purpose of handling it in a case when the data are collected from other than the owner. It also imposed safety measures to prevent sensitive information from being lost, stolen, breached, forged, altered, or damaged. The resident registration number handling authority was also tightened as restricted within presidential decrees, National Assembly Regulations, Supreme Court Regulations, Constitutional Court Regulations, Central Election Management Commission Regulations, and Board of Audit and Inspection Regulations. To prevent the illegal collection of personal information and reflect data usage increase in the big data era, the MOIS, the Korea Communications Commission, the MSIT, and the FSC had a joint announcement of

the 'Guidelines for De-identification of Personal Data' in June 2016, which supports de-identification measures for businesses with the help from special institutions in financial, medical, and public sectors. (However, the issues regarding the guideline were continuously raised, e.g., difficulty in utilizing personal information through de-identification due to lack of legal background, and later replaced by the guidelines for processing de-identification information.

In 2017, the government provided a standard on notational methods, e.g., size of the letter, and when a personal information handler receives the consent of the data owner by writing, important content should be indicated with ease such as sensitive personal information to collect and use. When the data owner requests perusal, correction, deletion, and suspension, the handler shall provide easy methods, e.g., telephone, e-mail, and internet, for the data owner to exercise rights easier.

In 2018, efforts to rationalize regulations on personal information protection to cope with environmental changes like the emergence of the fourth industrial revolution. To minimize confusion in the field, the government established the requirement and measures for the outsourcer and the outsourcee when outsourcing personal information handling to a third party (Article 26), and published the 「Personal Information Handling Entrustment Guide」 to provide explanations on frequently asked questions for businesses, such as conducting supervisory duties when entrusted to business abroad.

In 2020, the concept of 'de-identification' and 'de-identified information' was introduced to the 「Personal Information Protection Act」 to balance protection with the utilization of personal information, enabling the handling of de-identified information without consent from the owner, for the purpose of statistics, scientific research, and archive for the public. With this, the 「De-identification Information Handling Guideline」 was published for public guidance as well. With revising the 「Personal Information Protection Act Explanatory Book」, overall commentary on the 「Personal Information Protection Act」 was supplemented and an explanation on the matters amended by the Act was added.

In 2021, the government prepared the amendment bill to the 「Personal Information Protection Act」 and submitted to the National Assembly to strengthen the rights of information subjects in the digital age, such as the right to request transmission of

personal information and the right to respond to automated decisions. For the safe use of personal information in services based on the emerging ICT technologies (AI, biometric information, etc.), the government published the easy-to-understand 「Artificial Intelligence Personal Information Protection Self- Checklist」, which suggests 16 items to check and 54 items to identify that AI service developers and operators must check at all times for each stage of personal information processing. In addition, the government published the 「Biometric Information Protection Guideline」 that the biometric information handlers can understand easily and must follow for the safe use of biometric information at each stage of personal information processing. Besides, the 「Emergency Personal Information Processing and Regulations of Protection」 was established to classify personal information processing methods in emergencies into four emergencies and explain the personal information processing methods of related organizations by dividing them into the collection, use, and provision stages. Furthermore, by allowing legal guardians to quickly check CCTV in case of suspicion of child abuse at daycare centers, the inconvenience of guardians related to the complicated CCTV viewing procedures has been resolved.

2. Information and Communication Sector

In July 2014, related ministries including the KCC announced the 'Measures to reinstate personal information protection' to resolve public anxiety over personal information breaches and come up with comprehensive and fundamental personal information protection measures. In May 2015, the 「Standard for Technical and Managerial Safeguards of Personal Information」 was revised to enhance personal information protection by leading self-regulation for industry and reflecting environmental changes in ICT. 'Technical and managerial safeguards' include the installation and operation of access control devices such as intrusion prevention systems to block illegal access to personal information, security measures using cryptographic technology to safekeeping and transmit personal information, and measures to prevent a computer virus incident by installation and operation of anti-virus software.

In 2016, the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」was amended, and the main contents are as follows.

First, when smartphone application developers or companies need access authorization to users' smartphones, it is required to distinguish between the necessary and non-necessary (selective) authority to perform the primary functions of the program, and notify the users for clear acknowledgment of this and shall obtain users' consent.

Second, it is prohibited that smartphone application developers or companies allow the program unavailable to users who have disagreed with selective access authorization that are not essential to performing the primary functions of the program.

Third, in the case of outsourcing personal information handling, the outsourcer should provide education to the outsourcee.

Fourth, outsourcing personal information handling needs to be done by writing, and the outsourcee may re-outsource to a third party only with consent from the outsourcer.

Fifth, where a chief privacy officer becomes aware of any violation of this Act or other relevant laws concerning the protection of personal information, the chief privacy officer shall take corrective measures immediately, and shall report to the business owner, if necessary.

Sixth, a provision is introduced that enables confiscation/penalty for the redemption of the profit earned by personal information-related crimes, and punitive compensation for damage by a telecommunication service provider when personal information is lost, stolen, breached, forged, altered, or damaged.

In August 2016, the 「Personal Information Breach Response Manual」 was published for businesses can take quick action on the incident. This manual describes measures to mitigate the damage, with how to prevent additional breach incidents.

In February 2017, the KCC published the 「Online Personalized Advertising Privacy Guidelines」 to mitigate personal information incidents that occurred by an indiscreet collection of internet users' behavioral information and advertising.

In March 2017, the 「Smartphone App Personal Information Protection Guide」 was published to raise awareness and compliance with laws for related businesses, and in December of the same year, the 「Biological Information Protection Guideline」 was published for the protection and safe use of biological information.

The 「Standard Manual for Technical and managerial safeguards of Personal Information」 was revised that the businesses should follow for safekeeping and managing the personal information. The manual is revised with 10 provisions, the management part including establishment and implementation of an internal management plan, and the technical part including access control, prevention of forgery and alteration of the access log, personal information encryption, and prevention of malicious programs. The manual is added with a few changes, e.g., the purpose of protection measures, limiting the access time, and entities for encryption, reflected by the government notification revised in May 2015.

2018 was a year in which both voices of strengthening personal information protection and use of personal information, which is one of the key resources for the 4th industrial revolution, from many countries including Korea. It was a time that a harmony between the two demands is emphasized more than ever, that the KCC implemented diverse policies to harmonize personal information protection and policies for the 4th industrial revolution.

Telecommunication service providers with no address or business office in Korea but meet certain criteria, shall have a local representative, who shall perform the duties of the privacy officer, and submission of materials required to notify, report, and investigate a personal information breach incident. Korean people are allowed to exercise their right of self-determination practically to global businesses just as same as they do to local, e.g., withdrawal of consent for the collection, use, provision of personal information, and claim for perusal, and request for correction of personal information. When a material is requested to submit by the KCC to a global business to determine whether personal information was violated, shall be submitted promptly.

In the case of personal information which already had been transferred to a foreign country would be re-transferred to a third country, it is required to receive consent with the same principle applies to transferring overseas. Measures were, therefore, prepared to ensure the safe circulation of Koreans' personal information transferring to the countries with less protection than Korea and to protect equally under international norms. Users' and businesses' convenience is improved by expanding the tools for consent, e.g., text messaging, mobile apps, and social media, after a revision of the current 「Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」, which

limitedly enumerated to telephone and email in order to have users' consent on collecting and use personal information. The online personal information handling guideline is revised with the content including specific standards for business on users' rights, e.g., request for personal information perusal/provision, and access logs.

In 2019, with the amendment of the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」;

① Children's right is strengthened as information and communication service providers should use clear & easy-to-understand forms and languages when notifying children under the age of 14 regarding personal information handling,

② The KCC established policies to promote and support information and communication service providers for their autonomous personal information protection activities to increase their responsibility, and

③ Information and communication service providers that meet a specified scale are mandated to take necessary measures to assure relief on victims' damage caused by personal information incidents, e.g., subscribing to an insurance or mutual aid, and financial reserve.

In addition, by amending the 「Act on the Protection, Use, etc. of Location Information」 for using personal location information more safely while being protected, the entry regulation was eased by requiring the object location information provider to report to the KCC instead of obtaining permission. It also allowed micro-enterprises or one-person creative companies to carry out location-based service business through a simplified reporting process, which allowed location information handling without prior consent from the owner for object location information.

As such, the KCC strives to harmonize policy to support revitalizing data-based emerging industry in response to the 4th industrial revolution, having a basis of thorough protection of personal and location information.

In 2020, the KCC had a significant change in its tasks that the personal information protection for the information and communication sector is transferred to the Personal Information Protection Commission (PIPC) by the amendment of the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and the 「Personal Information Protection Act」. Provision

of personal information is deleted from the 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」, which are transferred into 'special cases concerning personal information handling by information and communication service providers' within the 「Personal Information Protection Act」 and are recognized as special only to those providers. This special provision includes that the information and communications service providers should notify/report breach incidents (within 24 hours), subscribe to an insurance or a mutual aid for liability on damage compensation, destroy the personal information of the user who is dormant for more than one year, notify access logs, and designate a local representative.

In 2021, an amendment to the 「Personal Information Protection Act」 was made (July 2021) to integrate the special regulations on personal information processing for information and communications service providers, etc. into the general regulations. This amendment was proposed to the National Assembly on September 28, 2021, after going through government legislative review and is currently pending.

Chapter 5

Cybersecurity for General Public

Section 1 Cybersecurity Consultation Service

1. Overview

The Korea Internet & Security Agency(KISA) started a service for information security complaints on January 18, 2020, through the '118 Counseling Center'. Previously, the KISA operated several centers for information security issues for malware, security incidents, personally identifiable information breaches, and unsolicited mail. The '118 Counseling Center' provides a unified report point for the public to file a complaint about information security issues

The KISA provides unified professional counseling 24/7 services free of charge so that complaints can consult any concerns in information security issues for malware, security incidents, personally identifiable information breaches, and unsolicited mail. Moreover, Internet users can ask online identities, questions about the Internet addresses, and others.

2. 118 Consultation Status

A. Annual consultation status

118 Counseling had gradually decreased since 2015 but has been on the rise again since 2018. In 2021, the number of telephones and online consultations received through the 118 Counseling Center was 405,971 decreasing 4.8% compared to 2020.

Table 3-5-1-1 Annual ☎118 Consultation Status

(Unit of measurement: cases)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Number of consultation	349,185	462,073	477,392	612,496	633,760	553,664	384,311	336,407	378,178	389,611	426,382	405,971

From the counseling cases in 2021, personally identifiable information ranks highest at 50.0%, malware and security incidents follow for 17.7%, and spam for 9.8%.

There were 202,923 cases of personally identifiable information in 2021, an 11.1% increase from the previous year. The text messages for the National Assembly elections and the rise of consultation about voice and messenger phishing impersonating public institutions and acquaintances caused it.

The number of reported malware and incident responses was 71,915, decreasing 8.1% from 2020. The decrease in the number of reported malware and incident responses seems to be caused by the decreased number of smishing messages of fraudulent medical checkups and emergency relief funds compared to the previous year.

Table 3-5-1-2 ☎118 Consultation status by field

(Unit of measurement: cases)

	2018	2019	2020	2021
Personal information	163,172	158,214	175,366	202,923
Spam	45,960	37,272	35,286	39,612
Hacking·Viruses	58,333	66,398	78,284	71,915
Others*	110,713	127,727	136,446	91,521
Total	378,178	389,611	426,382	405,971

* 'Others' refers to information on business-related inquiries of the KISA, such as online advertisement and electronic transaction dispute settlement, internet address, etc.

The number of reported spam was 39,612, and it increased by 12.3% from 2020. As the number of spam messages from overseas has recently increased in order to evade the domestic legal network, the consultations related to unsolicited emails and texts have also increased.

Section 2 Cybersecurity Awareness

1. 'Cybersecurity Day' Ceremony

In commemoration of the 10th Cybersecurity Day in 2021, the Ministry of Science and ICT (MSIT), the Ministry of Public Administration and Security, and the National Intelligence Service jointly hosted a commemorative ceremony online in July 14th. The government designated July as Cybersecurity Month, and the second Wednesday of July as the Cybersecurity Day to highlight the importance of cybersecurity as a basis of social safety, and gather cross-government response capacity and promote public interests.

The 2021 ceremony emphasized the importance of information security in the ongoing non-face-to-face society under the theme of 'Digital Safe Country through National Strategy for Cybersecurity in the Digital Age'. The 2021 ceremony created synergies such as sharing the latest information security issues and trends and promoting information security solutions by linking information security conferences, AI-speaker business agreements, and other additional events.

In order to prevent the spread of COVID-19, the 2021 ceremony went live online broadcast through systematic online transmission, and more than 7,000 people including industry, academia, research officials, and the public participated in the non-face-to-face ceremony.

Figure 3-5-2-1 The 10th 'Cybersecurity Day' ceremony

At the ceremony, the government awarded eight people and two groups for one order, two medals, three presidential commendations, and four prime minister's commendations in order to congratulate their contribution and endeavors to information security in Korea. The Minister of ICT awarded 21 Ministerial Citations (19 people and two groups) to those who contributed to the improvement of information security in Korea.

At the ceremony, a total of 20 lectures including the keynote speech were held in a non-face-to-face manner. Information security experts presented 18 presentations in three tracks and six sessions about information security trends and information protection policy trends, and issues of cybersecurity threat in the Non-Contact era. In the presentations, various information such as the latest information security technologies and trends and national policy tasks were shared, and Q&A and two-way communication were conducted using real-time online chatting.

Moreover, 20 information security companies participated in the information security product exhibition operated for one month in July on the official website of the 'Cybersecurity Day' to promote information security products and services and provide consultation.

2. Activities to raise awareness of national cybersecurity

In the era of Non-Contact, teleworking and remote class became the new standard and cyber threats for the new environment. As a result, ransomware damage for monetary gain increased rapidly, but public awareness did not reach this level. Accordingly, the government tried to raise national cybersecurity awareness by carrying out various activities that are related to the spread of public attention and voluntary online cybersecurity practice.

In connection with the Cybersecurity Month, the government conducted a citizen participatory information security practice campaign under the theme of preventing ransomware damage on social media and used mass media (radio, subway, KTX, etc.) to increase the promotion effect. At the same time, the government produced educational videos related to information security careers for elementary, middle, and high school students and posted them on a highly useful educational site (Career Net).

Figure 3-5-2-2 PR activities related to awareness-raising

3. Financial cybersecurity awareness

A. Financial Security Course for C-level executives and guest CEO of financial company Seminars.

Since 2017, the Financial Security Institute (FSI) has operated the Financial Security Advanced Course for C-level Executives to cultivate the CISO's capabilities and create a venue for discussion and communication.

Moreover, the FSI launches the 'CEOs of financial company invitation seminar' to raise financial cybersecurity awareness for the CEO, CISO, CDO, and CIO. In 2020*, the FSI invited 33 CEOs and 54 executives of financial and fintech companies to strengthen communication with major financial and fintech companies and raise

financial security awareness.

* Due to the spread of COVID-19, it was not held in 2021.

B. Financial Information Security Conference

The FISCON (Financial Information Security Conference) is the most significant cybersecurity event in the financial sector. It is co-hosted by the FSI, the Financial Information Security Association, and the Financial Security Forum and sponsored by the Financial Services Commission and the Financial Supervisory Service.

In 2021, FISCON held an offline event under the theme of 'Digital Platform Era, Financial Security Challenges and Future Strategies', and provided lectures on a total of 21 topics including related policies and technologies in the digital financial innovation era, in which the financial platform business becomes active in earnest.

Figure 3-5-2-3 **FISCON 2021**

Chapter 6

International Cooperation

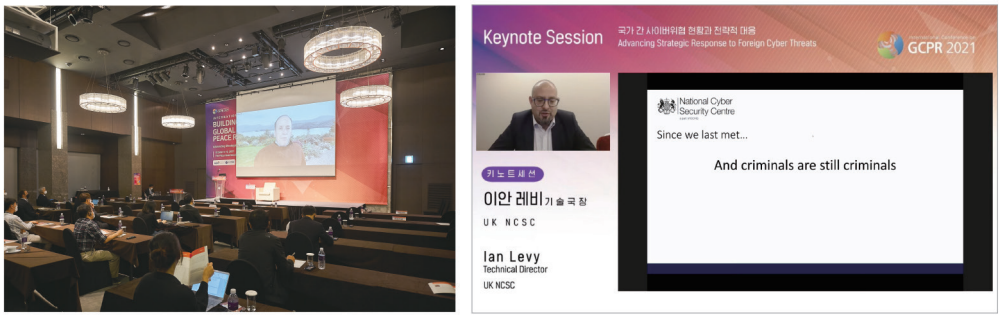
Section 1 Cybersecurity Diplomatic Activities

1. International Conference on Building Global Cyberspace Peace Regime

On October 5, 2021, the National Security Research Institute (NSR) and the National Intelligence Service (NIS) held the 'International Conference on Building Global Cyberspace Peace Regime (GCPR)' under the theme of 'Current Status of Cyber Threats and Strategic Response'. At this academic conference, which was the 6th conference since 2014, experts from cyber security legislation, policy, and technology discussed countermeasures for cyber threats in the international community.

This conference discussed national response strategies on state-involved malicious cyber activities. About 30 local and foreign experts participated online and offline to discuss the evolution of international cyber threats, the evaluation of the severity of foreign cyberattacks and cases of response strategies, and the direction of Korea's response strategy as key agenda.

Figure 3-6-1-1 The 6th International Conference on Building a Global Cyberspace Peace Regime



2. Discussion on UN International Cybersecurity Norms

The international community has continued its efforts to establish international norms within the United Nations (UN) to counter cross-border cyber threats that have emerged as a major challenge to national security.

In 2018, the Korean government participated in the Open-Ended Working Group (OEWG), a consultative body under the 1st Committee of the 73rd UN General Assembly. And, in March 2021, the Korean government contributed to the consensus adoption of the 1st OEWG report that includes the threat posed by the misuse of ICT technology, the need to protect key infrastructure, the application of existing international laws to cyberspace, and the importance of trust-building and capacity building. Besides, as the 2nd OEWG for the term of 2021-2025 has started operating in December 2021, the government will work closely with the international community to actively participate in discussions on the formation of international norms to create secure cyberspace.

Furthermore, as a co-sponsor, the Korean government is participating in the Program of Action for Responsible State Behaviors (PoA), which was launched to strengthen the capacity of developing countries to implement the norms agreed upon in the UN Group of Governmental Experts (GGE) report. The Korean government is also working hard to officially launch the PoA and expand its scope.

3. Regional multilateral cybersecurity international cooperation

With the 2017 ASEAN Regional Forum (ARF) Foreign Ministers' Meeting, the Korean government is participating in the ICT Security Inter-Sessional Meeting (ISM), which was established to discuss cybersecurity Confidence Building Measures (CBM). At the 3rd ICT Security ISM held in April 2021, the Korean government assumed the co-chairs of the meeting along with Indonesia, Australia, and Russia. Therefore, by 2023, the Korean government will contribute to strengthening regional cybersecurity capabilities and developing CBM.

The Korean government regularly holds cybersecurity conferences in cooperation with the Organization for Security and Co-operation in Europe (OSCE) to promote cyber trust-building cooperation. In June 2021, the 3rd Korea-OSCE Cybersecurity Conference was held under the theme of 'Cybersecurity Cooperation in the Asia-Europe Region'. At this conference, more than 300 people, including officials from governments and international organizations in the Asia-Europe region, as well as related academics and industry figures, shared various opinions and best practices related to cybersecurity and had in-depth discussions on cybersecurity cooperation between regions.

In addition, the Korean government participated in the 'Ransomware Response Initiative' hosted by the US National Security Council (NSC) in October 2021. By doing so, the Korean government consulted with other major countries to seek countermeasures against ransomware, which has recently emerged as a critical cyber threat. About 30 countries including the United Kingdom, Germany, Canada, Australia, New Zealand, Singapore, Japan, Dominican Republic, and Kenya participated in the meeting to respond to discuss specific ways to cooperate and respond to ransomware such as network security and resilience, countermeasures against illegal financial activities, ransomware network blocking, and diplomatic measures.

4. Cyber Policy Consultation for Bilateral Cooperation in Cybersecurity

Since the Korea-US Cyber Policy Consultation was held in 2012, the Korean government has been holding the cyber policy consultation with 12 countries including the United States, China, Japan, and Russia, as well as the EU and NATO.

These cyber policy consultations serve as a useful opportunity for countries to share cybersecurity-related strategies, policies, and threat information, and to strengthen cybersecurity-related cooperation.

Under the 'MOU on Cyber and Critical Technology Cooperation' signed on the occasion of the Korea-Australia Foreign Affairs and Defense Ministers' Meeting in September 2021, the Korean government held the 1st ROK-Australia Cyber and Critical Technology Policy Dialogue in December of the same year. The government also held the 1st Korea- Netherlands Cyber Policy Consultation in December to discuss the ways to establish a network and promote cooperation between the cybersecurity-related organizations of the two countries.

5. World Emerging Security Forum

In 2021, the government established the World Emerging Security Forum to respond to new security threats such as the spread of COVID-19, expansion and diversification of cyber threats, and development, misuse and abuse of new technologies beyond human control, and to lead the international order of solidarity and cooperation.

The 1st World Emerging Security Forum was held in Seoul on November 16-17, 2021. Not only government officials from major countries such as the United States, China, Russia and France, but also international organizations, academia, and business experts participated in the forum as speakers. They explored the ways to raise awareness and strengthen cooperation with the international community to respond to new security threats such as health security, cybersecurity, and new technology security.

Figure 3-6-1-2 The 1st World Emerging Security Forum

6. Support for capacity building in developing countries

Since cyber threats often originate from or via countries that lack cybersecurity capabilities, developing countries need to strengthen their cybersecurity capabilities.

The Korean government, together with the Korea International Cooperation Agency (KOICA) and related organizations, cooperated with the Hanoi University of Science and Technology in Vietnam through an Inclusive Business Solution (IBS) and promoted a cybersecurity manpower training project (USD 1.15 million) from 2019 to 2021. Furthermore, the government is carrying out the following Official Development Assistance (ODA) projects: strengthening Indonesia's cybercrime investigation capacity from 2018 to 2023 in cooperation with the National Police Agency and the National Forensic Service (USD 5.1 million), reinforcement of cyber investigation capabilities for the Nepal National Police Agency's Cyber Security Bureau from 2021 to 2026 (USD 8 million).

In August 2021, the Korean government and the Netherlands jointly held a seminar on the 'application of international law in cyberspace'. At the seminar, the Korean government exchanged opinions on the application of international law in cyberspace and shared best practices with 50 officials in the field of cybersecurity from 14 Asian countries, including ASEAN.

In addition, in December 2021, the government announced the 'Memorandum of Understanding on a ROK-Australia Digital Cooperation Initiative in Southeast Asia' to jointly develop the Korean government's New Southern Policy, which promotes strengthening cooperation between Korea and Southeast Asian countries, and Australia' Indo-Pacific agenda.

Section 2 International Cybersecurity Cooperation

1. Cybersecurity Alliance for Mutual Progress

In July 2016, the KISA launched the Cybersecurity Alliance for Mutual Progress (CAMP) participated by related agencies and Computer Emergency Response Teams (CERT) from other countries to strengthen bilateral cooperation and respond to the growing demand for multilateral cooperation. As of December 2021, the CAMP has grown to a networking platform to secure cyberspace and build trust and consists of 62 member organizations from 47 countries. It regularly publishes newsletters to share member countries' current status in cybersecurity. In 2021, the CAMP shared the current status of member organizations' activities and response strategies during the digital transition period due to the COVID-19, as well as, the current status and prospects of cybersecurity in member countries. In addition, the CAMP published four newsletters, including the introduction of new cybersecurity regulations and each member organization's capacity-building activities.

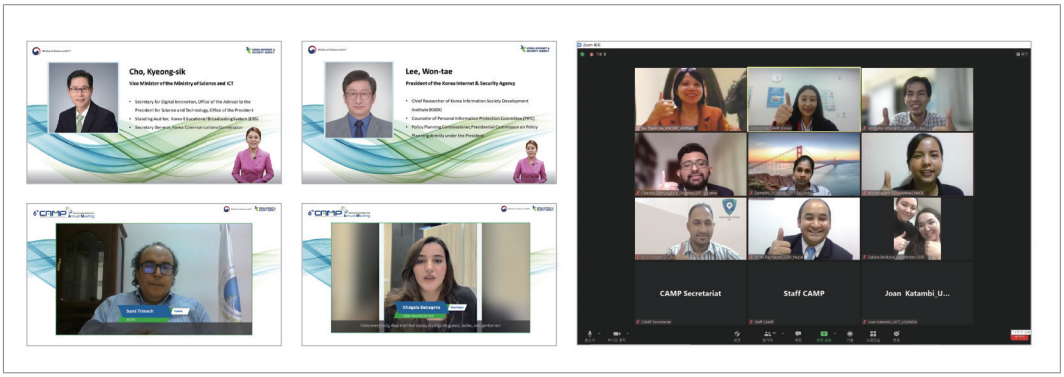
In October 2021, 16 organizations from 14 countries participated in the annual general meeting of the CAMP held as the second online video conference following the 2020 online meeting due to the continued spread of COVID-19. During the general meeting, in addition to sharing cybersecurity trends led by the digital transformation, seminars and online exhibition halls were operated for export assistance to companies whose overseas PR activities have been contracted due to the COVID-19, and to promote the technologies and products of excellent local cybersecurity vendors.

In November of the same year, a regional forum was held with Fiji's 'Safer Internet Centre' and Sri Lanka's CERT to promote a network among CAMP members in the

Asia-Pacific region. At this forum, the CAMP members shared the latest trends in cybersecurity in the region and discussed ways to strengthen cooperation between the CAMP Council and the Asia-Pacific region.

In addition, the CAMP organizes the Steering Committee and holds regular meetings to discuss and lead operational issues centered on members. After the inauguration of CAMP, the KISA was elected as the chairperson and secretariat, and was re-elected in 2019 and will be active until 2022. Besides, as of 2021, the KISA is currently serving as a steering committee member.

Figure 3-6-2-1 CAMP 6th Annual General Meeting (Left), CAMP Regional Forum (Right)

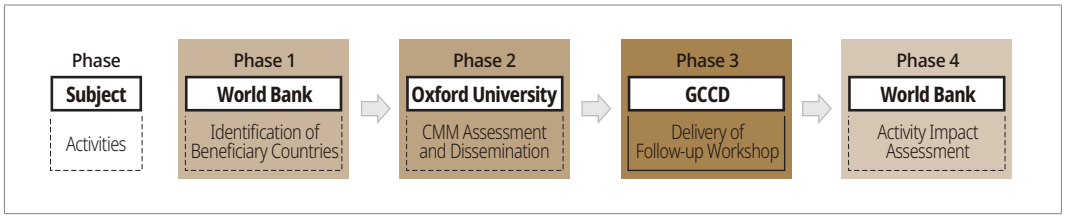


2. Cybersecurity Capacity Building

The MSIT and the KISA operate the Global Cybersecurity Center for Development (GCCD) to enhance the global cybersecurity environment by strengthening the cybersecurity capacity of developing countries. The GCCD has capacity-building programs for developing countries that share cybersecurity experiences and the know-how of Korea. In 2020, the GCCD held online seminars on cybersecurity based on the cybersecurity needs and preferences of cooperating partners. A total of 189 people from Asia and Africa participated in the non-face-to-face capacity-building webinar with four topics: cybersecurity policy, personal information security, information security certification system, and operation of CERT. Moreover, the GCCD operated new technology practice programs based on virtual environments on topics such as web security, network security, and infringement incident response by region.

The KISA is participating in a joint project in collaboration with the World Bank and Oxford University. The World Bank identifies demands from developing countries, and Oxford University assesses the necessity for strengthening the cybersecurity capacity of the country, and based on the assessment results, GCCD provides customized follow-up workshops, based on Cybersecurity Capacity Maturity Model (CMM).

Figure 3-6-2-2 CMM follow-up Workshop



The KISA participated in the 1st CMM joint project from 2016 to 2018. And, in 2019, KISA launched the 2nd joint project from 2019 to 2021 and hosted the follow-up cybersecurity workshop for Kosovo, Serbia, and 4 Caribbean countries: Dominica, Grenada, St. Lucia, and Saint Vincent and Grenadines.

The KISA will continue bilateral and multilateral global cooperation activities, and invite experts from local cybersecurity vendors in the private sector to capacity building programs so that they can promote their excellent technologies and products to global partner organizations, for the sake of securing global-level capabilities and continue export assistance to local companies.

3. Global Activities of the Computer Emergency Response Team (CERT)

Many countries, including Korea, are operating a CERT (Computer Emergency Response Team) with national responsibilities to deal with cyber incidents. International communities are to quickly respond to large-scale cyber incidents and national CERTs communicate constantly through the forum: The Forum of Incident Response Security Teams (FIRST) was formed in 1990 with most of the members from the United States and Europe, and the Asia-Pacific Computer Emergency Response Teams (APCERT) was formed in 2003 by Asia Pacific countries including Korea and Japan.

As of 2021, more than 600 teams from private and public sectors and 99 individuals have FIRST membership. The Korea Computer Emergency Response Team Coordination Center (KrCERT/CC) in the KISA has been participating in FIRST conferences since 1996 on behalf of the private sector in Korea and became the first Asian team to acquire full membership in 1998. The other members in Korea are, SK infosec, AhnLab, National Cyber Security Center, Korea Education and Research Information Service, Financial Security Institute, Igloo Security, NAVER Business Platform, the National Information Resources Service (NIRS), the Ministry of Trade, Industry and Energy Cyber Security Center, and NHN (in the order of membership approval).

The APCERT has 33 operational member teams from 24 economies and 12 partner teams. The KrCERT/CC has been a Steering Committee member since its establishment in 2003 and contributed to member expansion strengthening credibility among existing members as a convener and a steering committee member of the Membership Working Group, which manages APCERT's membership qualifications and operating rules. Furthermore, KrCERT/CC successfully moderated the APCERT international joint exercise in 2021 with the topic of countering spear phishing targeting the telecommuting environment.

2022 **National Cybersecurity White Paper**

Published on August 2022

Published by National Intelligence Service, the Ministry of Science and ICT, the Ministry of Interior and Safety, the Personal Information Protection Commission, the Financial Services Commission, and the Ministry of Foreign Affairs

Contributed by Korea Internet & Security Agency, the National Security Research Institute, and the Financial Security Institute